TORSION POINTS ON HYPERELLIPTIC JACOBIAN VARIETIES

by
HAMİDE SULUYER

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Doctor of Philosophy

Sabancı University
June 2025

ABSTRACT

TORSION POINTS ON HYPERELLIPTIC JACOBIAN VARIETIES

HAMİDE SULUYER

MATHEMATICS Ph.D DISSERTATION, June 2025

Dissertation Supervisor: Assoc. Prof. Dr. Mohammad Sadek

Keywords: Hyperelliptic Curve, Jacobian, Torsion Order, Continued Fractions, Modular Curve

This thesis presents a detailed study of explicit methods for constructing hyperelliptic curves over the rationals with new torsion orders on the Jacobian. We mention two methods for this purpose.

First, we utilize the relation between hyperelliptic curves and continued fractions of power series. We find that for any integer N in the interval $[3g, 4g+1]$, $g \geq 3$, satisfying specific partition constraints, there exist infinitely many families of Jacobians of hyperelliptic curves of genus g possessing a rational torsion point of order N. We found some original examples of 1-parameter families of hyperelliptic curves. For example, hyperelliptic curves of genus 3 with the Jacobian possessing torsion divisor of order 13, genus 4 with order 15, genus 5 with order 17, 18, and 21.

In the second part, we present another method to construct hyperelliptic curves for which the Jacobians contains a torsion divisor of order quadratic in genus g. For any integer $g \geq 2$, we construct hyperelliptic curves of genus g over $\mathbb{Q}$ whose Jacobian varieties contain rational torsion points of order N where $N = 4g^2 + 2g - 2$, respectively $4g^2 + 2g - 4$. These curves introduce previously unobserved quadratic torsion orders and provide new torsion orders. For example, rational torsion points in the Jacobians of hyperelliptic curves of genus 4 with torsion order 70, and genus 3 with torsion order 20.

In the last chapter we work on elliptic curves. It was established which groups can occur as torsion subgroups of elliptic curves over quartic number fields. Except for some higher-order groups, we identify the quartic field with the smallest absolute discriminant such that an elliptic curve over this field has the given torsion.

ÖZET

HİPERELİPTİK JACOBİYEN ÇOKLUKLARININ TORSİYON NOKTALARI

HAMİDE SULUYER

MATEMATİK DOKTORA TEZİ, HAZİRAN 2025

Tez Danışmanı: Doç. Dr. Mohammad Sadek

Anahtar Kelimeler: Hipereliptik Eğri, Jakobiyen, Torsiyon Mertebesi, Sürekli Kesirler, Modüler Eğri

Bu tez, Jacobiyende yeni torsiyon mertebelerine sahip olan rasyoneller üzerinde hipereliptik eğriler inşa etmek için açık yöntemlerin ayrıntılı bir çalışmasını sunar. Bu amaçla iki methoddan bahsedeceğiz.

Öncelikle, hipereliptik eğriler ile sürekli kesirler arasındaki ilişkiyi kullanıyoruz. $[3g, 4g+1]$ aralığındaki herhangi bir $N \in \mathbb{Z}$ için, ve cins $g \geq 3$ için, belirli bölüm kısıtlamalarını sağlayan, mertebesi N olan torsiyon noktasına sahip bir parametreli, cinsi g olan hipereliptik Jacobiyen ailesi bulmayı başardık. 1 parametreli hipereliptik eğri ailesinin bazı orijinal örneklerini bulduk. Örneğin, cinsi $g = 3$ olan ve, mertebesi 13 torsiyona sahip hipereliptik Jacobiyen, cinsi $g = 4$, olan ve, mertebesi 15 torsiyona sahip hipereliptik Jacobiyen, cinsi 5 Jakobiyeni torsiyon mertebesi $17, 18$ ya da 21 olan eleman içeren hipereliptik eğri aileleri bulduk.

İkinci bölümde, Jacobiyenlerin g cinsinde ikinci dereceden bir torsiyon eleman içerdiği hipereliptik eğriler oluşturmak için bir yöntem sunuyoruz. Herhangi bir tam sayı $g \geq 2$ için, $\mathbb{Q}$ üzerinde, Jacobiyen çoklukları sırasıyla $N = 4g^2 + 2g - 2$, ve $4g^2 + 2g - 4$ olan rasyonel torsiyon elemanları içeren g cinsli hipereliptik eğriler oluşturuyoruz. Bu eğriler daha önce gözlemlenmemiş ikinci dereceden torsiyon mertebelerini tanıtır ve yeni torsiyon mertebeleri sağlar. Örneğin, cins 4, mertebe 70, cins 3 mertebe 20.

Son bölümde eliptik eğriler üzerine çalışıyoruz. Kuartik sayı cisimleri üzerindeki eliptik eğrilerin torsiyon alt gruplarının sınıflandırılması biliniyor. Yüksek dereceden gruplar hariç olmak üzere, verilen torsiyona sahip bir eliptik eğrinin tanımlandığı, diskriminantının mutlak değeri en küçük olan kuartik sayılar cismini belirliyoruz.

ACKNOWLEDGEMENTS

I owe my deepest thanks to my thesis advisor Assoc. Prof. Dr. Mohammad Sadek. His patience, clear guidance, ability to direct me to the right sources, deep expertise, and constant understanding played a central role in making this work. I feel incredibly fortunate to have had the opportunity to work with such an advisor.

I would like to extend special thanks to Prof. Dr. Ekin Özman and Asst. Prof. Dr. Ayesha Qureshi for their support during my progress evaluations and for their valuable feedback throughout that process. I am also grateful to the esteemed members of my thesis jury, Prof. Dr. Ferruh Özbudak and Assoc. Prof. Dr. Ayberk Zeytin, for taking the time to read my work in detail and for their insightful comments and suggestions, which significantly contributed to the improvement of this dissertation.

I would like to express my sincere gratitude to Sabancı University for the financial support provided during my Ph.D. studies. I am also thankful to the faculty members of Sabancı University for their valuable teaching and academic guidance throughout my time there. During my Ph.D. studies, the faculty members and friends at Sabancı University provided invaluable support during challenging times and created an environment that always felt welcoming and warm.

I am especially grateful to all the professors in the Department of Mathematics at Galatasaray University, who taught me mathematics and helped me discover my passion for it. They played an essential role in my academic and personal growth.

I would also like to thank my colleagues and professors at Atılım University for their support and collaboration during this period.

I am lucky to have friends who supported and encouraged me throughout this long journey, and I thank them sincerely.

Finally, I would like to thank my family and my beloved husband Hasan Suluyer. Their unwavering support, love, and belief in me have been my greatest source of strength.

To my family

TABLE OF CONTENTS

LIST OF FIGURES

1. Introduction

The Mordell-Weil theorem states that if an abelian variety A is defined over a number field K, then the group $A(K)$ of K-rational points on A is a finitely generated abelian group. An elliptic curve E over a number field K is an abelian variety with dimension 1. There is a group structure on the set of K-rational points, $E(K)$, of the elliptic curve given by the so-called chord-tangent process. In particular, we know that $E(K)$ is a finitely generated abelian group.

The classification of torsion points on elliptic curves over $\mathbb{Q}$ was completed by Mazur in 1978, providing a list of all possible torsion orders for elliptic curves defined over rationals in [Mazur & Goldfeld (1978)]. If $E/\mathbb{Q}$ is an elliptic curve, then the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups: A cyclic group $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, 3, \ldots, 10, 12$, or a product of two cyclic groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 1, 2, 3, 4$. Mazur's work shows that the torsion subgroup of any elliptic curve over $\mathbb{Q}$ can only have certain orders, which are restricted to a finite set of integers. Following this work, the classification of torsion points of elliptic curves over quadratic, cubic and quartic number fields has been completed, see the papers [Kamienny (1992), Kenku & Momose (1988), Jeon, Kim & Schweizer (2004), Derickx & Najman (2024)].

Later, the study of torsion points was expanded to Jacobians of higher-genus curves, particularly hyperelliptic curves. These curves, which have genus $g \geq 2$, exhibit more possibilities for the torsion structures compared to elliptic curves. Unfortunately, there is no group law given by the chord-tangent process on the set of K-rational points of these curves, unlike elliptic curves. Here, the group structure is obtained thanks to an abelian variety, which is called the Jacobian of the curve. A primary focus in this area of research has been to identify small genus hyperelliptic curves over $\mathbb{Q}$ whose Jacobians contain torsion divisors of orders that do not appear in the elliptic curve case over $\mathbb{Q}$. So in this case, the earliest significant result was the identification of genus 2 hyperelliptic curves with torsion points of order 11 or 13. These are the smallest torsion orders that do not occur for elliptic curves over $\mathbb{Q}$. The first examples of one-parameter family of genus 2 hyperelliptic curves that

contain torsion points of order 11 or 13 can be found in [Flynn (1991),Bernard, Leprévost & Pohst (2009)].

Moreover, the study of torsion points on Jacobians of genus 2 hyperelliptic curves has progressed significantly, with many researchers providing further examples of one-parameter families of hyperelliptic curves over $\mathbb{Q}$ that have torsion points of much larger orders. These include torsion points of orders such as 21, 22, 23, 25, 26, 27, 29, and beyond, see the papers [Leprévost (1991), Leprévost (1995), Leprévost (1997)]. The exploration of these large torsion orders has opened new directions for research, contributing to a deeper understanding of the arithmetic of hyperelliptic curves and their Jacobians.

The primary focus of our initial work in this thesis is to identify small genus hyperelliptic curves over $\mathbb{Q}$ that possess torsion orders that do not occur for elliptic curves over $\mathbb{Q}$, much like the discovery of Flynn and Leprévost of genus 2 hyperelliptic curves with torsion divisors of order 11 and 13. Additionally, our work may also involve the exploration of hyperelliptic curves that are not isomorphic to the curves constructed by Flynn and Leprévost, thus providing new examples of hyperelliptic curves of genus 2, 3, or other small values with the same torsion structures that are not isomorphic to the ones in their findings.

The thesis [Nicholls (2018)] provides a comprehensive classification of the possible orders of torsion divisors on the Jacobians of hyperelliptic curves of genus $2, 3$ and 4, as found in the current literature. We have constructed new hyperelliptic curves, as well as a one-parameter family of hyperelliptic curves, which exhibit different torsion orders for small genus g. To make this construction, we used two different methods.

Chapter 2 contains a preliminary section in which we introduce key definitions and fundamental theorems that are considered essential for the comprehension of the thesis.

In Chapter 3, we present the first method for constructing hyperelliptic curves. Here we use the relation between the order of the infinity divisor of the Jacobian of a hyperelliptic curve given by $y^2 = f(x)$ and the continued fraction expansion of y.

It is conjectured by Flynn that, there exists a constant c such that for every integer $g \geq 1$, and for every integer N satisfying $N < cg$, there exists a hyperelliptic curve defined over $\mathbb{Q}$ of genus g whose Jacobian is endowed with a rational torsion point of order N, see [Flynn (1990)]. This result suggests the existence of a family of hyperelliptic curves with rational torsion points of orders bounded linearly by the genus g. This conjecture is proved in [Leprévost (1996)], with $c = 3$. In this chapter

we extended this bound by using a different tool from the ones in Leprévost's paper. In this study, we demonstrate that for any integer N in the interval $[3g, 4g+1]$ with $g \geq 3$, satisfying specific partition constraints, there exist infinitely many families of hyperelliptic Jacobians possessing a rational torsion point of order N.

Theorem 1.1 *Fix an integer $g \geq 3$. Let $\alpha, \beta \geq 1, \gamma \geq 0$ be integers such that $2\alpha + 2\beta + \gamma = g+1$. Let $a_1(x), r(x), u(x) \in \mathbb{Q}[x]$ be of degrees α, β, γ, respectively. If the affine equation*

$$y^2 = r(x)^2 \Big(u(x)(a_1(x)^2 r(x) + 1) + a_1(x)\Big)^2 + 4\Big(u(x)a_1(x)r^2(x) + r(x)\Big)$$

describes a hyperelliptic curve C, then the divisor at infinity is torsion of order $g + 1 + 6\alpha + 3\beta + \gamma$.

In this chapter, we found some original examples of 1-parameter family of hyperelliptic curves of genus 3 with the Jacobian containing a torsion divisor of order 13, genus 4 with order 15, genus 5 with torsion divisor of order 17, 18, or 21.

In chapter 4, we present another method to construct the hyperelliptic curves. In chapter 3, using the continued fraction expansion method, we obtain torsion orders that are linear as a polynomial in the genus g. Here, our aim is to obtain a torsion divisor of order quadratic in g. In the literature, we have some papers that manage to find different quadratic torsion orders. For any even integer $g \geq 2$, Flynn provided a detailed construction of hyperelliptic curves of genus g defined over $\mathbb{Q}$, whose Jacobian varieties contain rational torsion points of order N, where N lies in the interval $\Big[g^2 + 2g + 1, g^2 + 3g + 1\Big]$, see [Flynn (1991)].

Additionally, Leprévost presented hyperelliptic curves of genus g whose Jacobians feature torsion points of order $2g^2 + 2g + 1$ or $2g^2 + 3g + 1$ in [Leprévost (1992)], and in [Leprévost (1997)] the Jacobians also include torsion points of orders $2g^2 + 4g + 1$ or $2g(2g+1)$, with possible orders of these points being N, $\frac{N}{2}$, or $\frac{N}{4}$, where $N = 2g^2 + 5g + 5$.

For any integer $g \geq 2$, we present hyperelliptic curves of genus g over $\mathbb{Q}$ such that their jacobian varieties contain a rational torsion point of order N where

$$N = 4g^2 + 2g - 2, \text{ respectively } 4g^2 + 2g - 4$$

These represent quadratic orders that have not been previously observed in the literature and provide us with new rational torsion orders of hyperelliptic Jacobian varieties that were previously undiscovered.

Theorem 1.2 *Fix an integer $g \geq 2$. We set $t_g = 1/(g^2(g-1))$ and $s_g = 1/(g(g-1)^2)$. We consider the following curves of genus g defined over $\mathbb{Q}$ by the equations*

$$\begin{aligned} C_{g,g-1} &: y^2 = f_{t_g}(x) := A_{g-1}(x)^2 - 4t_g x^{2g}(x-1), \\ C_{g,g-2} &: y^2 = f_{s_g}(x) = A_{g-2}(x)^2 - 4s_g x^{2g-1}(x-1)^2, \end{aligned}$$

where

$$\begin{aligned} A_{g-1}(x) &= \frac{(x-g)x^{g-1} + (x-1)^g + t_g x^2(x-1)\left((x-g)x^{g-1} - (x-1)^g\right)}{(x-g)}, \\ A_{g-2}(x) &= \frac{(x-g)x^{g-1} + (x-1)^g + s_g x(x-1)^2\left((x-g)x^{g-1} - (x-1)^g\right)}{(x-g)}. \end{aligned}$$

There is a torsion divisor on the curve $C_{g,g-1}$, respectively $C_{g,g-2}$, whose order is $4g^2+2g-2$, respectively $4g^2+2g-4$.

Consequently, we construct the new torsion orders in literature of a genus 4 hyperelliptic curve over $\mathbb{Q}$ whose jacobian has a torsion point of order 70, and a genus 3 hyperelliptic curve whose jacobian has a torsion point of order 20. Furthermore, for every integer $g \geq 2$, we give a 1-parameter family of hyperelliptic curves of genus g over $\mathbb{Q}$ whose Jacobian varieties possess a rational torsion point of order $2g^2+7g+1$.

In the last chapter, we work on elliptic curves. Assume that $y^2 = f(x)$ defines an elliptic curve where $\deg(f(x)) = 4$. In [Adams & Razar (1980)], it was proved that the continued fraction expansion of $\sqrt{f(x)}$ is periodic if and only if $D_\infty = \infty_1 - \infty_2$ is a torsion point. Moreover it was proved that if the order of D_∞ is N then the period of the continued fraction of $\sqrt{f(x)}$ is $N-1$ if N is odd, $N-1$ or $2(N-1)$ if N is even. Based on Adams and Razar's theorem and Mazur's classification of $E_{\text{tor}}(\mathbb{Q})$, the possible periods of $\sqrt{f(x)}$ are: $\{1,2,3,4,5,6,7,8,9,10,11,14,18,22\}$.

Van der Poorten listed all square-free quartic polynomials $f(x)$ over $\mathbb{Q}$ with a square leading coefficient, where the continued fraction expansion of $\sqrt{f(x)}$ is periodic, showing that no $\sqrt{f(x)}$ has periods 9 or 11, see [van der Poorten (2004)]. Sadek [Sadek (2016)] extended this to quadratic fields, identifying all possible periodic continued fraction expansions of $\sqrt{f(x)}$ over the quadratic fields K, and showed that all these periods occur over some quadratic fields.

We similarly investigated the possible periods of $\sqrt{f(x)}$ over cubic number fields.

Finally, it is known which groups appear as torsion for infinitely many non-isomorphic elliptic curves over cubic number fields. This set is denoted by S.

Moreover, for all but two groups in S, Filip Najman identified a cubic field with the smallest absolute value of discriminant over which there exists an elliptic curve having that group as its torsion subgroup in [Najman (2012)].

It is established which groups can occur as torsion groups of elliptic curves over quartic number fields, in [Derickx & Najman (2024)]. For every possible torsion subgroup arising from the group of points on an elliptic curve defined over a quartic number field, we identify the quartic field with the smallest absolute value of the discriminant. To find these quartic number fields, we examine the arithmetic properties of modular curves $X1(m, mn)$ where $m, n \geq 1$. We look for the points of each modular curve over the quartic number fields K in increasing order of $|\Delta(K)|$. For each field, we either find an elliptic curve with the specified torsion group or prove that no such curve exists. We mostly use Magma [Bosma, Cannon & Playoust (1997)], to compute the Mordell-Weil group of the given modular curves $X_1(m, mn)$ if they are elliptic curves or, if they are hyperlliptic curves we compute the points by putting a bound. For the higher genus non- hyperelliptic curves we have tried some methods to decide non-existence of the torsion order over a quartic number field. However, we couldn't find an explicit method to decide the existence of the torsion order over a number fields for these curves.

2. Background

Sections 1 and 2 of the theoretical background discussed here is adapted from the book [Silverman (2009)].

2.1 Affine Varieties and Projective Varieties

2.1.1 Affine Varieties

The n-dimensional **affine space** $A^n = A^n(K)$ is a space which consists of all n-tuples of elements from a field K. An element $P = (a_1, \ldots, a_n)$ from the affine space A^n represents a point in A^n over K.

Let $K[X_1, \ldots, X_n]$ be the ring of polynomials in n variables over K. A subset $V \subseteq A^n$ is called an **algebraic set** if there is a set $M \subseteq K[X_1, \ldots, X_n]$ such that:

$$V = \{P \in A^n \mid F(P) = 0 \text{ for all } F \in M\}.$$

For an algebraic set $V \subseteq A^n$, the set of polynomials given as follows

$$I(V) = \{F \in K[X_1, \ldots, X_n] \mid F(P) = 0 \text{ for all } P \in V\}$$

is called the **ideal of** V. This ideal is an ideal in $K[X_1, \ldots, X_n]$, and it can be generated by finitely many polynomials $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Then, we can express V as:

$$V = \{P \in A^n \mid F_1(P) = \cdots = F_r(P) = 0\}.$$

An algebraic set $V \subseteq A^n$ is called **irreducible** if it cannot be written as the union of two proper algebraic subsets V_1 and V_2. That is, V is irreducible if and only if the corresponding ideal $I(V)$ is a prime ideal. **An affine variety** is an irreducible algebraic set $V \subseteq A^n$.
The coordinate ring of an affine variety V is the quotient ring $\Gamma(V) = K[X_1, \ldots, X_n]/I(V)$. Since $I(V)$ is a prime ideal, $\Gamma(V)$ is an integral domain. For every element $f = F + I(V) \in \Gamma(V)$, we define a function $f : V \to K$ by setting:

$$f(P) := F(P) \text{ for } P \in V.$$

The quotient field $K(V) = \text{Quot}(\Gamma(V))$ is called the field of rational functions (or the function field) of V. It contains K as a subfield. The dimension of V is the transcendence degree of $K(V)/K$.

For a point $P \in V$, we define the local ring at P as:

$$O_P(V) = \{f \in K(V) \mid f = \frac{g}{h}, g, h \in \Gamma(V), h(P) \neq 0\}.$$

This is a local ring with quotient field $K(V)$, and its unique maximal ideal is:

$$M_P(V) = \{f \in K(V) \mid f = \frac{g}{h}, g, h \in \Gamma(V), h(P) \neq 0, g(P) = 0\}.$$

For $f = \frac{g}{h} \in O_P(V)$ with $h(P) \neq 0$, the value of f at P is defined by:

$$f(P) := \frac{g(P)}{h(P)}.$$

2.1.2 Projective Varieties

On the set $A^{n+1} \setminus \{(0, \ldots, 0)\}$, we may define an equivalence relation $\sim$ by:

$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n)$ if and only if there exists a nonzero $\lambda \in K$ such that $b_i = \lambda a_i$ for all $i \in \{0, \ldots, n\}$.

The equivalence class of $(a_0, a_1, \ldots, a_n)$ with respect to $\sim$ is denoted by $(a_0 : a_1 : \cdots : a_n)$. The n-dimensional **projective space** $\mathbb{P}^n = \mathbb{P}^n(K)$ is the set of all equivalence

classes:

$$\mathbb{P}^n = \{(a_0 : \cdots : a_n) \mid a_i \in K, \text{ not all } a_i = 0\}.$$

An element $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n$ is a point, and the coordinates $a_0, \ldots, a_n$ are referred to as the homogeneous coordinates of P.

A monomial of degree d is a polynomial $G \in K[X_0, \ldots, X_n]$ of the form:

$$G = a \prod_{i=0}^{n} X_i^{d_i}, \quad \text{where } a \neq 0 \in K \text{ and } \sum_{i=0}^{n} d_i = d.$$

A polynomial F is called **homogeneous** if it is the sum of monomials of the same degree. An ideal $I \subseteq K[X_0, \ldots, X_n]$ generated by homogeneous polynomials is called a **homogeneous ideal**.

Let $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n$ and let $F \in K[X_0, \ldots, X_n]$ be a homogeneous polynomial. We say that $F(P) = 0$ if $F(a_0, \ldots, a_n) = 0$, which is well-defined because for any $\lambda \neq 0$, we have:

$$F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d F(a_0, \ldots, a_n),$$

where d is the degree of F. Thus, $F(a_0, \ldots, a_n) = 0 \iff F(\lambda a_0, \ldots, \lambda a_n) = 0$.

A subset $V \subseteq \mathbb{P}^n$ is called **projective algebraic set** if there exists a set of homogeneous polynomials $M \subseteq K[X_0, \ldots, X_n]$ such that:

$$V = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ for all } F \in M\}.$$

The ideal $I(V) \subseteq K[X_0, \ldots, X_n]$, which is generated by all homogeneous polynomials F such that $F(P) = 0$ for all $P \in V$, is called the ideal of V. This is a homogeneous ideal. A projective algebraic set $V \subseteq \mathbb{P}^n$ is irreducible if and only if $I(V)$ is a homogeneous prime ideal in $K[X_0, \ldots, X_n]$. A projective variety is an irreducible projective algebraic set.

Given a non-empty variety $V \subseteq \mathbb{P}^n$, we define its homogeneous coordinate ring as:

$$\Gamma_h(V) = K[X_0, \ldots, X_n]/I(V),$$

which is an integral domain containing K. An element $f \in \Gamma_h(V)$ is said to be a form of degree d if $f = F + I(V)$ for some homogeneous polynomial $F \in K[X_0, \ldots, X_n]$

with $\deg F = d$. The function field of V is defined by:

$$K(V) := \left\{ \frac{g}{h} \mid g, h \in \Gamma_h(V) \text{ are forms of the same degree and } h \neq 0 \right\},$$

which is a subfield of $\mathrm{Quot}(\Gamma_h(V))$, the quotient field of $\Gamma_h(V)$. The dimension of V is the transcendence degree of $K(V)$ over K.

Let $P = (a_0 : \cdots : a_n) \in V$ and $f \in K(V)$. Write $f = \frac{g}{h}$ where $g = G + I(V)$ and $h = H + I(V)$ are forms of degree d with homogeneous polynomials G and H of degree d. Since:

$$\frac{G(\lambda a_0, \ldots, \lambda a_n)}{H(\lambda a_0, \ldots, \lambda a_n)} = \frac{\lambda^d G(a_0, \ldots, a_n)}{\lambda^d H(a_0, \ldots, a_n)} = \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)},$$

we define $f(P) := \frac{G(a_0,\ldots,a_n)}{H(a_0,\ldots,a_n)}$ if $H(P) \neq 0$. The ring $O_P(V) = \{f \in K(V) \mid f \text{ is defined at } P\}$ is a local ring with maximal ideal:

$$M_P(V) = \{f \in O_P(V) \mid f(P) = 0\}.$$

2.2 Arithmetic of Elliptic Curves

Elliptic curves are nonsingular algebraic curves of genus one having a specified base point, which is called the point at infinity and denoted by ∞. In general, we are writing an elliptic curve in the following form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Moreover the point at infinity is $\infty = (0 : 1 : 0)$ and $a_1, \cdots, a_6 \in K$ for some field K. Elliptic curves can be written in the different forms and usually, people use Weierstrass form, it can be obtained by changing the coordinates $x = X/Z$ and $y = Y/Z$, and we obtain the following equation :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

If the characteristic of the algebraic closure $\overline{K}$ is not 2, we can simplify the equation by completing the square. To achieve this, we perform the substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3),$$

which transforms the equation into the following form:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where the new coefficients are defined as

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Additionally, we introduce the following quantities:

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_1^4,$$

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_3^2 + 36b_2b_4 - 216b_6,$$

$$\Delta = -b_2^2b_8 - 8b_3^4 - 27b_2^6 + 9b_2b_4b_6,$$

$$j = \frac{c_4^3}{\Delta}, \quad \omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

It can be verified that the following relations hold:

$$4b_8 = b_2b_6 - b_2^4$$

and

$$1728\Delta = c_4^3 - c_2^6.$$

Δ is discriminant of the curve and j is the j-invariant of the curve.

Assuming that the characteristic of K is neither 2 nor 3, the elliptic curves we are considering are described by the short Weierstrass equation:

$$E : y^2 = x^3 + Ax + B.$$

For this equation, we define the discriminant Δ and the j-invariant as follows:

$$\Delta = -16(4A^3 + 27B^2), \quad j = \frac{-1728(4A)^3}{\Delta}.$$

The only transformation that preserves the form of this equation is the change of

variables:

$$x = u^2 x' \quad \text{and} \quad y = u^3 y'$$

for some $u \in \overline{K}^*$, and under this transformation, we have

$$u^4 A' = A, \quad u^6 B' = B, \quad u^{12}\Delta' = \Delta.$$

Proposition 2.1 *(a) A short Weierstrass equation has the following properties:*

(i) The curve is nonsingular if and only if $\Delta \neq 0$.

(ii) The curve has a node if and only if $\Delta = 0$ *and* $c_4 \neq 0$.

(iii) The curve has a cusp if and only if $\Delta = c_4 = 0$.

(b) Two elliptic curves are isomorphic over $\overline{K}$ *if and only if their* j*-invariants are equal.*

(c) For any $j_0 \in \overline{K}$*, there exists an elliptic curve defined over the field* $K(j_0)$ *with* j*-invariant equal to* j_0.

Proposition 2.2 *Every elliptic curve defined over a field* K *can be described by a Weierstrass form.*

Note that the Weierstrass form is commonly used, it is not the only classical form for representing elliptic curves.

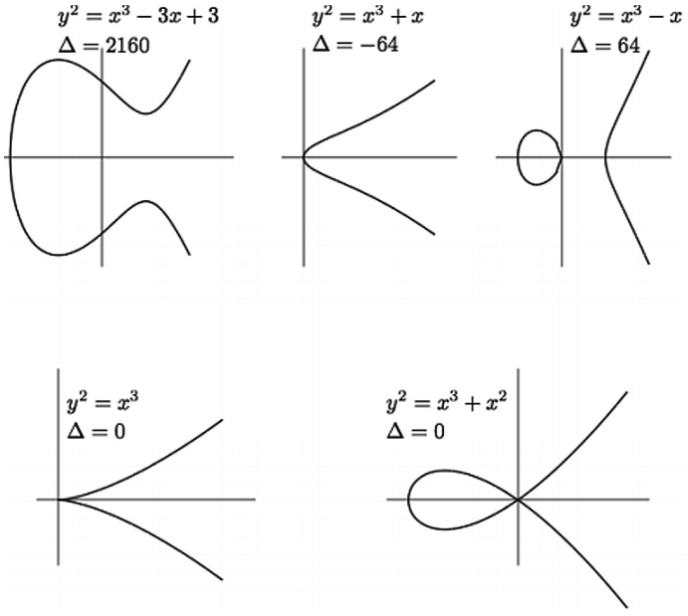

Figure 2.1 The first three curves are examples of elliptic curves, while the fourth curve exhibits a cusp, and the fifth curve displays a node.

2.2.1 Group Law

Assume that E is an elliptic curve defined over the field K. Then E can be described by a Weierstrass equation. Thus, the set of K-rational points of the elliptic curve E is given by

$$E(K) = \{(x,y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

The main advantage of elliptic curves lies in the fact that an addition operation can be defined on this set, which can be thought of as a special form of addition, which is a chord tangent process, and through it, we demonstrate that the set of K-rational points, $E(K)$, actually possesses a group structure.
The curve $E \subset \mathbb{P}^2$ consists of the points $P = (x,y)$ that satisfy the Weierstrass equation, along with the point at infinity $\infty = (0:1:0)$. Take $L \subset \mathbb{P}^2$ a line and since the equation of elliptic curve has degree three, the line L intersects E at exactly three points, counting with multiplicities, which is coming from the Bézout's theorem.

Next, we define a composition law $\oplus$, that is a special addition law on the elliptic curves, on E as follows:
Let P, $Q \in E$, and let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P). Let R be the third point of intersection of L with E. Let L' be the line through R and ∞. Then L' intersects E at three points: R, ∞, and a third point, which we denote by $P \oplus Q$.

Proposition 2.2. The composition law (III.2.1) satisfies the following properties:

(a) If a line L intersects E at the points P, Q, and R (not necessarily distinct), then

$$(P \oplus Q) \oplus R = \infty.$$

(b) For every point $P \in E$, we have

$$P \oplus \infty = P.$$

(c) The composition law is commutative, i.e.,

$$P \oplus Q = Q \oplus P \quad \text{for all } P, Q \in E.$$

(d) For any point $P \in E$, there exists a point $-P \in E$ such that

$$P \oplus (-P) = \infty.$$

(e) The composition law is associative, meaning that for any points $P, Q, R \in E$,

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

In other words, the composition law (III.2.1) makes E into an abelian group with identity element ∞. Furthermore:

(f) Suppose E is defined over K. Then the set of K-rational points of an elliptic curve E given by $E(K)$ forms a subgroup of E.

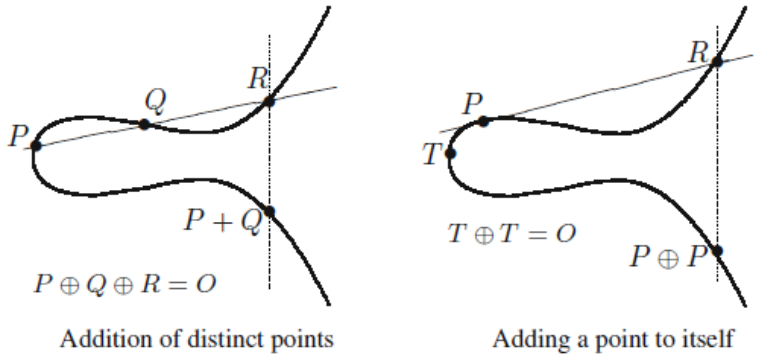

Figure 2.2 The figures give us composition law. In these figures O represents the point at infinity, ∞.

We now simplify the notation by dropping the special symbol $\oplus$ and use the standard group operations "+" to represent the group law on an elliptic curve E. For $n \in \mathbb{Z}$ and a point $P \in E$, we define:

$$[n]P = P + \cdots + P \quad n > 0, \text{ addition of } n \text{ many P}$$

$$[n]P = -P - \cdots - P, \quad n < 0, \text{ addition of } |n| \text{ many -P}$$

$$[0]P = \infty$$

Even if we can explain the group law on the graph of an elliptic curve we can give the explicit formula for the group operation on E. Consider E, an elliptic curve given by the Weierstrass equation:

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

and let $P_0 = (x_0, y_0) \in E$. We can explain the coordinates of the inverse of this point. To compute $-P_0$, we draw the line L through P_0 and the identity point ∞, finding the third intersection with E. The line L is given by:

$$L : x - x_0 = 0.$$

Substituting into the equation for E, we find the quadratic polynomial $F(x_0, y)$ has roots y_0 and y_0', where $-P_0 = (x_0, y_0')$. Then we have the following equalitys:

$$F(x_0, y) = c(y - y_0)(y - y_0') = y^2 + a_1 x_0 y + a_3 y - x_0^3 - a_2 x_0^2 - a_4 x_0 - a_6$$

From the coefficients of y^2 we obtain $c = 1$ and by equating the coefficients of y we obtain $y_0' = -y_0 - a_1 x_0 - a_3$. Finally we have:

$$-P_0 = (x_0, -y_0 - a_1 x_0 - a_3).$$

For the addition law, let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E. If $x_1 = x_2$ and $y_1 + y_2 + a_1 x_2 + a_3 = 0$, we have $P_1 + P_2 = \infty$, see the previous explanation. Otherwise, the line L through P_1 and P_2 (or the tangent line when $P_1 = P_2$) is given by:

$$L : y = \lambda x + \nu.$$

The relation between the points is:

$$P_1 + P_2 + P_3 = \infty.$$

We substitute this into the equation of E to find the third intersection point $P_3 = (x_3, y_3)$;

$$\begin{aligned} F(x, \lambda x + \nu) &= x(x - x_1)(x - x_2)(x - x_3) \\ &= (\lambda x + \nu)^2 + a_1 x(\lambda x + \nu) + a_3(\lambda x + \nu) - x^3 - a_2 x^2 - a_4 x - a_6 \end{aligned}$$

By looking the coefficients of x^3, we get $c = -1$. By coefficients of x^2 we get $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, and since P_3 is a point on the line L, $y_3 = \lambda x_3 + \nu$. Here $P_1 + P_2 + P_3 = \infty$, then $P_1 + P_2 = -P_3$. We need to apply the inverse formula to P_3. Hence $-P_3 = (x_3, -x_3(\lambda + a_1) - \nu - a_3)$.

Group Law Algorithm

Let E be an elliptic curve given by:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

(a) Let $P_0 = (x_0, y_0)$. Then:

$$-P_0 = (x_0, -y_0 - a_1 x_0 - a_3).$$

(b) For $P_1 + P_2 = P_3$ with $P_i = (x_i, y_i) \in E$ for $i = 1, 2, 3$:

- If $x_1 = x_2$ and $y_1 + y_2 + a_1 x_2 + a_3 = 0$, then $P_1 + P_2 = O$.
- If $x_1 = x_2$

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, \quad \nu = \frac{-x_3^2 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$$

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

- Otherwise, define λ and ν by:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

The equation of the line through P_1 and P_2 is:

$$y = \lambda x + \nu.$$

Using these, $P_3 = P_1 + P_2$ has coordinates:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

(c) Special cases include for $P_1 \neq \pm P_2$:

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

and the duplication formula for $P = (x, y) \in E$:

$$x[2]P = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6}.$$

Example 2.1 *To compute $P + P$ for the point $P = (1, 3)$ on the curve $y^2 = x^3 + 8$, we first calculate the λ and ν for the case $x_1 = x_2$. Using the formulas for x_3 and y_3, we find that $x_3 = \frac{-7}{4}$ and $y_3 = \frac{-13}{8}$. Therefore, $P + P = \left(\frac{-7}{4}, \frac{-13}{8}\right)$.*

Example 2.2 *On the elliptic curve $y^2 = x^3 - 5x$, add the points $P = (-1, 2)$ and $Q = (0, 0)$. Using the formula, we find that the slope λ is:*

$$\lambda = \frac{0-2}{0-(-1)} = \frac{-2}{1} = -2.$$

Then, we calculate x_3 and y_3:

$$x_3 = (-2)^2 - (-1) - 0 = 4 + 1 = 5,$$
$$y_3 = (-2)(-1-5) - 2 = (-2)(-6) - 2 = 12 - 2 = 10.$$

Thus, $P + Q = (5, 10)$. We can easily verify that the sum is a point on the curve.

Theorem 2.1 ***(Mordell-Weil)***
Let K be a number field and let E/K be an elliptic curve. The group $E(K)$ is a finitely generated abelian group. That is,

$$E(K) \cong \mathbb{Z}^r \times E(K)_{tors}$$

$\mathbb{Z}^r$ represents the free part of the group, that is, it consists of the infinite order points. The invariant r is the rank, the number of independent points of infinite order. The rank r is more difficult to compute. There is no general algorithm. Descent methods can sometimes estimate it. In the literature, relatively little is still known about r.

$E(K)_{\text{tors}}$ is the torsion subgroup of $E(K)$. It consists of points of finite order. The torsion subgroup is finite. Its structure is well known:

$$E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \quad \text{or} \quad E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

The situation we described for the rank is not valid for the torsion subgroup. There are many studies on this topic in the literature. The classification of the torsion subgroup for an elliptic curve over rational numbers $\mathbb{Q}$ has been fully determined by Mazur in [Mazur & Goldfeld (1978)]. Furthermore, the complete classification for the number fields of degree $2, 3, 4$, was given in [Kamienny (1992), Kenku & Momose (1988), Jeon et al. (2004), Derickx & Najman (2024)], which is generalized by Mazur's theorem. Research in this area is still ongoing today.

Theorem 2.2 (Mazur & Goldfeld (1978)) *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:*

- $\mathbb{Z}/N\mathbb{Z}$ *with* $1 \leq N \leq 10$ *or* $N = 12$,
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *with* $1 \leq N \leq 4$.

Further, each of these groups occurs as $E_{tors}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

Moreover, Merel proved a general theorem for the torsion subgroup of an elliptic curve.

Theorem 2.3 (Merel (1996)) *For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields $K/\mathbb{Q}$ of degree at most d, and all elliptic curves E/K, we have:*

$$E_{tors}(K) \leq N(d).$$

2.3 Arithmetic of Hyperelliptic Curves

The following background information is summarized from the work of Michael Stoll [Stoll (2014)]. For further details, see [Stichtenoth (2009)].

2.3.1 Hyperelliptic Curve

Definition 1 *Let k be a field. Fix $g \in \mathbb{N} \setminus \{0\}$. The weighted projective plane $\mathbb{P}^2_g$ is the set of the equivalence classes of triples (α, β, γ) where the equivalence is given as follows :*

$$(\alpha, \beta, \gamma) \simeq (\alpha', \beta', \gamma') \text{ if and only if } (\alpha', \beta', \gamma') = (\lambda\alpha, \lambda^{g+1}\beta, \lambda\gamma), \text{ for some } \lambda \in k.$$

For $g = 0$ we obtain the definition of the standard projective plane. There is a one-to-one correspondence between the affine space $\mathbb{A}^2(k)$ and $\mathbb{P}^2_g$ given as follows:

$$\begin{aligned} \mathbb{P}^2_g &\longrightarrow \mathbb{A}^2(k) \\ (\alpha : \beta : \gamma) &\longmapsto \left(\tfrac{\alpha}{\gamma}, \tfrac{\beta}{\gamma^{g+1}}\right) \text{ where } \gamma \neq 0 \end{aligned}$$

$$\begin{aligned}\mathbb{A}^2(k) &\longrightarrow \mathbb{P}^2_g \\ (\alpha,\beta) &\longmapsto (\alpha:\beta:1)\end{aligned}$$

In the similar way, we obtain a bijection between the points with $\alpha \neq 0$ and $\mathbb{A}^2(k)$ given by

$$\begin{aligned}\mathbb{A}^2(k) &\longrightarrow \mathbb{P}^2_g \\ (\beta,\gamma) &\longmapsto (1:\beta:\gamma)\end{aligned}$$

These two subsets of $\mathbb{P}^2_g$ can be called as **the two standard affine patches of** $\mathbb{P}^2_g$.

Definition 2 *Let $g \geq 2$ be an integer. A **hyperelliptic curve** is a subvariety of the weighted projective plane $\mathbb{P}^2_g$ given by the equation $y^2 + H(x,z)y = F(x,z)$; where H and F are homogeneous of degrees $g+1$ and $2g+2$, respectively, and $F \in k[x,z]$ is homogenous of degree $2g+2$ and squarefree. If $\mathrm{char}(k) \neq 2$ then a hyperelliptic curve can be defined in the form $y^2 = F(x,z)$, such that F satisfies the same conditions. We define the set of k-rational points of the curve as follows:*

$$C(k) = \{(\alpha:\beta:\gamma) \in \mathbb{P}^2_g(k) \mid \beta^2 = F(\alpha,\gamma)\}.$$

If we intersect C with the affine patches of $\mathbb{P}^2_g$, we obtain the standard affine patches of C. They are affine plane curves and they are given as follows:

$$y^2 = F(x,1) \quad \text{and} \quad y^2 = F(1,z),$$

respectively. During this thesis, we will write $C : y^2 = f(x) := F(x,1)$, but we will always consider C as a projective curve. Let $C : y^2 = F(x,z)$ and $(\alpha:\beta:\gamma) \in C(k)$ such that $\gamma \neq 0$ have the form $(\alpha:\beta:1)$ where $\beta^2 = f(\alpha)$. These points correspond to the solutions in k of the equation $y^2 = f(x)$. We will frequently just write (α,β) for such an affine point. Meanwhile, we have other k-rational points with $\gamma = 0$. These points on C are called the **points at infinity**.

We obtain them by taking $z = 0$ and $x = 1$ in the defining equation, $F(x,z) = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1}z + \ldots + f_1 x z^{2g+1} + f_0 z^{2g+2}$.

- If $f_{2g+2} = 0$ then that gives us deg $f = 2g+1$, and there is one such point, namely $(1:0:0)$. We denote this point by ∞.

- If $f_{2g+2} = s^2$ is a nonzero and square in k, then there are two k-rational points at infinity, namely $(1:s:0)$ and $(1:-s:0)$. We will denote them by ∞_1 and

∞_2. Otherwise there are no k-rational points at infinity.

Example 2.3 *The curve given by* $C : y^2 = x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1$ *is a hyperelliptic curve on rational numbers* $\mathbb{Q}$.

The degree of the polynomial on the right-hand side is 6, so the genus g *of this curve is 2.*

At infinity, there are two points $\{(1:-1:0), (1:1:0)\}$ *as the degree of* $f(x)$ *is even. The set of all rational points on the curve is given as follows:*

$$C(\mathbb{Q}) = \{(1:-1:0), (1:1:0), (0:-1:1), (0:1:1), (-1:-1:1), (-1:1:1)\}.$$

The most popular theorem about the set of the k- rational points of any curve is given as follows:

Theorem 2.4 (Faltings (1986)) *Let* C/k *be a smooth curve of genus* $g \geq 2$. *Then* $C(k)$ *is finite.*

2.3.1.1 Divisors, Picard Group, Jacobian of the Curve

Definition 3 *Consider the hyperelliptic curve* $C : y^2 = F(x, z)$ *of genus* g *over a field* k. *The* ***coordinate ring*** *of the curve* C *over* k *is defined as the quotient ring:*

$$k[C] := k[x, y, z]/\langle y^2 - F(x, z)\rangle.$$

Here, the ideal $\langle y^2 - F(x, z)\rangle$ *is generated by the relation* $y^2 = F(x, z)$, *which is irreducible and homogeneous. Thus,* $k[C]$ *is an integral domain.*
The field $k(C)$, *which is the field of fractions of* $k[C]$, *consists of rational functions on the curve* C *over* k. *It is called the* ***function field*** *of* C *over* k.

Definition 4 *Let* k *be a number field and* $\bar{k}$ *be its algebraic closure. Let* C *be a smooth, projective and absolutely irreducible curve over a field* k. *A* ***divisor*** D *on* C *is a finite formal integral linear combinations of points in* $C\left(\bar{k}\right)$. *In other words,*

$$D = \sum_{P \in C(\bar{k})} n_P \cdot P$$

where $n_P \in \mathbb{Z}$ *and* $n_P = 0$ *for all but finitely many points* P.

- *The degree of such a divisor is* $\deg(D) = \sum_{P \in C(\bar{k})} n_P$.

- *The set of divisors is called the divisor group which is a free abelian group and denoted by* Div_C.

- *The degree zero divisors form a subgroup of the divisor group* Div_C*, which is denoted by* Div_C^0.

- D *is called an effective divisor, if the non-zero terms* n_P *are positive integers (i.e.,* $n_P > 0$ *for all* P*).*

Let k be a number field and $\bar{k}$ be its algebraic closure. $\bar{k}(C)$ is the function field of C over $\bar{k}$.

Definition 5 *Let* $\phi \in \bar{k}(C)^\times$*. We define the divisor of* ϕ *to be*

$$\mathrm{div}(\phi) = \sum_P ord_P(\phi) \cdot P$$

where $ord_P(\phi) \geq 0$ *if* P *is the zero of* ϕ *and gives us the multiplicity of* P*. But if* P *is the pole of* ϕ *then* $ord_P(\phi) \leq 0$*. We call such a divisor* ***principal divisor****. We write* Princ_C *for the set of principal divisors which is a subgroup of* Div_C.

Definition 6 *The quotient group* $\mathrm{Pic}_C = \mathrm{Div}_C / \mathrm{Princ}_C$ *is called the* ***Picard group of*** C*. We say two divisors* D*,* D' *are linearly equivalent if and only if* $D - D'$ *is principal; we denote it as* $D \sim D'$.

Example 2.4 *Let* $C : y^2 = f(x)$*. If* $\deg f = 2g+2$ *then the divisors of the functions* x *and* y *over the curve can be given as follows:*

- $\mathrm{div}(x) = (0, \sqrt{f(0)}) + (0, -\sqrt{f(0)}) - \infty_1 - \infty_2$
- $\mathrm{div}(y) = \sum_{\alpha : f(\alpha)=0} (\alpha, 0) - (g+1)(\infty_1 + \infty_2)$

If $\deg(f) = 2g+1$ *then then the divisors generated by the functions* x *and* y *over the curve can be given as follows:*

- $\mathrm{div}(x) = (0, \sqrt{f(0)}) + (0, -\sqrt{f(0)}) - 2\infty$
- $\mathrm{div}(y) = \sum_{\alpha : f(\alpha)=0} (\alpha, 0) - (2g+1) \cdot \infty$

Example 2.5 *Let $a_1, a_2, a_3 \in \bar{k}$ such that $a_i \neq a_j$, for $i \neq j$, where k is a field, and* $\mathrm{char}(k) \neq 2$. *We have the following curve:*

$$C : y^2 = (x - a_1)(x - a_2)(x - a_3).$$

C is a smooth curve with a single point at infinity because $\deg(f) = 3$. *For $i = 1, 2, 3$, let $P_i = (a_i, 0) \in C$. Then*

$$\begin{aligned} \mathrm{div}(x - a_i) &= 2P_i - 2\infty \\ \mathrm{div}(y) &= P_1 + P_2 + P_3 - 3\infty \end{aligned}$$

Proposition 2.3 *Let C be a smooth curve and let $f \in \bar{k}(C)^*$.*

i. $\mathrm{div}(f) = 0$ *if and only if $f \in \bar{k}^*$.*

ii. $\deg(\mathrm{div}(f)) = 0$.

It follows that Princ_C is the subgroup of Div^0_C. Then one defines

$$\mathrm{Pic}^0_C = \mathrm{Div}^0_C \,/\, \mathrm{Princ}_C .$$

Note that if k is a field, then k^{sep} refers to the subfield of the algebraic closure of k which contains the elements that are separable over k; this field called the *separable closure* of k.

Theorem 2.5 *Let C be a smooth, projective and absolutely irreducible curve of genus g over the field k. Then there exists an abelian variety J, called the* ***Jacobian*** *of the curve C, of dimension g over k such that for each field $k \subset L \subset k^{sep}$, we have $J(L) = \mathrm{Pic}^0_C(L)$.*

Theorem 2.6 ***(Mordell-Weil Theorem)*** *Let k be a number field and let J be the Jacobian of a curve over k. Then the group $J(k)$ is a finitely generated abelian group, i.e.*

$$J(k) \simeq \mathbb{Z}^r \times J_{tor}(k)$$

where r is the rank of the group, representing its free part, and $J_{tor}(k)$ is the torsion subgroup of $J(k)$ which consists of elements of finite order.

Let P_0 be a rational point on the curve C over k, we define the following map

$$i_{P_0} : C \longrightarrow J(k)$$

$$P \longmapsto [P - P_0]$$

This morphism is injective when the genus $g > 0$. Hence, the problem of determining the set of k-rational points on C, denoted by $C(k)$, can be equivalently reformulated as finding the intersection $J(k) \cap i(C)$. This formulation allows us to utilize the group structure of J to extract information about $C(k)$. Then we can say that even though there is no group structure on hyperelliptic curves unlike elliptic curves, there is a group law on the Jacobian of the curve. In literature, there is still limited understanding regarding the rank. However, in the case of hyperelliptic curves, there is no general classification for the torsion order, similar to the case of elliptic curves. Even when considering the field $\mathbb{Q}$, we do not have a classification or a bound on the possible torsion orders.
Over finite fields, there is a well-known theorem that provides an estimate for the number of rational points on hyperelliptic curves as follows:

Theorem 2.7 ***(Hasse-Weil Bound)*** *Let C be a smooth, absolutely irreducible projective curve of genus g over a finite field $\mathbb{F}_q$. The number of rational points $N = |C(\mathbb{F}_q)|$ satisfies:*

$$|N - (q+1)| \leq 2g\sqrt{q}.$$

The following theorem helps finding torsion subgroups of Jacobians of hyperelliptic curves over $\mathbb{Q}$.

Definition 7 *A prime p is said to be a prime of good reduction for C if the reduction of C modulo p remains a smooth curve. The reduction map ρ_p takes a point in $J(\mathbb{Q})$, the Jacobian of C over the rationals, and maps it to $\overline{J}(\mathbb{F}_p)$, the Jacobian of the reduction of C modulo p over the finite field $\mathbb{F}_p$.*

Theorem 2.8 *Let C be a hyperelliptic curve over $\mathbb{Q}$, and let J denote its Jacobian. Let p be a prime of good reduction for C. Then the reduction map $\rho_p : J(\mathbb{Q}) \to \overline{J}(\mathbb{F}_p)$ induces an injective group homomorphism on the torsion subgroup $J(\mathbb{Q})_{tors}$.*

Definition 8 *Let C be a smooth, projective, absolutely irreducible curve over a field k, and let D be a divisor in $\mathrm{Div}_C(k)$. The **Riemann-Roch space** associated with the divisor D is the k-vector space given as follows:*

$$L(D) = \left\{\varphi \in k(C)^{\times} : div(\varphi) + D \geq 0\right\} \cup \{0\}.$$

Here, $\mathrm{div}(\varphi)$ denotes the divisor of the rational function φ. The space $L(D)$ consists of those rational functions φ whose divisor, when added to D, is a non-negative divisor.

Theorem 2.9 ***(Riemann-Roch Theorem)***

Let C be a smooth, projective, absolutely irreducible curve of genus g over a field k. Then there exists a divisor $W \in \mathrm{Div}_C(k)$ such that for every divisor $D \in \mathrm{Div}_C(k)$, the dimension of the Riemann-Roch space $L(D)$ is finite. Additionally, the following formula holds:

$$\dim_k L(D) = \deg D - g + 1 + \dim_k L(W - D).$$

In particular, if $\dim_k L(W) = g$, and the degree of W is $\deg W = 2g - 2$, then

$$\dim_k L(D) = \deg D - g + 1.$$

for $\deg D \geq 2g - 1$

Example 2.6 *Consider a hyperelliptic curve $C : y^2 = f(x)$ of odd degree and genus g.*

Using the equation of the curve, we can eliminate powers of y greater than the first power, which simplifies the structure of $k[x, y]$. This ring has a k-basis consisting of the elements:

$$\{1, x, x^2, \ldots, y, xy, x^2y, \ldots\}.$$

We know that the valuation at ∞ for x is $ord_\infty(x) = -2$ and the valuation at ∞ for y it is $ord_\infty(y) = -(2g + 1)$. This means the valuation of x^n is $ord_\infty(x^n) = -2n$, and the valuation of $x^n y$ is $ord_\infty(x^n y) = -(2n + 2g + 1)$.

Thus, the valuation at the point at infinity ∞ for any linear combination of these basis elements is determined by the element with the minimal valuation among those with nonzero coefficients. Then we obtain the following Riemann-Roch spaces for the divisor obtained by integer multiple of point at infinity, ∞.

$$L(0) = \langle 1 \rangle,$$

$$L(\infty) = \langle 1 \rangle,$$

For $n \leq g$,

$$L(2n \cdot \infty) = \langle 1, x, x^2, \ldots, x^n \rangle,$$

For $n < g$,

$$L((2n+1)\cdot\infty) = \langle 1, x, x^2, \ldots, x^n \rangle,$$

For $n = g$,

$$L(2g\cdot\infty) = \langle 1, x, x^2, \ldots, x^g \rangle,$$

For $n = g+1$,

$$L((2g+1)\cdot\infty) = \langle 1, x, x^2, \ldots, x^g, y \rangle,$$

For $n \geq g+1$,

$$L((2n)\cdot\infty) = \langle 1, x, x^2, \ldots, x^g, y, x^{g+1}, xy, \ldots, x^{n-g-1}y, x^n \rangle.$$

For $n \geq g$,

$$L((2n+1)\cdot\infty) = \langle 1, x, x^2, \ldots, x^g, y, x^{g+1}, xy, \ldots, x^n, x^{n-g}y \rangle.$$

We defined a map from the set of points of a hyperelliptic curve defined over a field k and the Jacobian of the curve over k. Now the following theorem gives us the representation of points on the Jacobian.

Theorem 2.10 *Let C be the genus g hyperelliptic curve given by $y^2 = f(x)$ with degree of $f(x)$ being $2g+1$. Fix a rational point $P_0 \in C(k)$. For each point $Q \in J(k)$, there is a unique effective divisor $D_Q \in \mathrm{Div}_C(k)$ of minimal degree such that*

$$Q = [D_Q - (\deg D_Q)\cdot P_0]$$

Furthermore, we have $\deg D_Q \leq g$, where g is the genus of the curve.

2.4 Continued Fractions and Order of The Infinity Divisor

Let $y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$ with $\deg(f(x)) = 2g+2$ for $g \geq 2$ is the genus of the curve. Then we have two points at infinity, as we discussed in the previous section, which are given by ∞_1 and ∞_2. The infinity divisor is given by $D_\infty = \infty_1 - \infty_2$ that is an element of the Jacobian of the curve, $\mathrm{Jac}(\mathbb{Q})$. In this section we will see the relation between the continued fraction expansion of $y = \sqrt{f(x)}$ and the order of the infinity divisor.

2.4.1 Continued Fractions

In this section, we briefly summarize the main results on classical continued fractions and continued fractions of power series. See works such as [Nicol & Petersen (2023), Hardy & Wright (1979)] for general references on continued fractions.
For any positive real number $\alpha \in \mathbb{R}$, one can give the continued fraction expansion as follows:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$

where a_n are positive integers, referred to as the partial quotients. The rational numbers $\frac{p_n}{q_n}$, where p_n and q_n are coprime positive integers, are defined as:

$$\frac{p_n}{q_n} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \frac{1}{a_n}}}$$

These are called convergents. The sequence of these rational numbers approximates α with an error of $\frac{1}{q_n^2}$. Specifically, for all n, the approximation satisfies:

$$\left| \alpha - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n^2}$$

Example 2.7 *The continued fraction expansion of* $\sqrt{2}$ *is given as follows:*

$$\begin{aligned}
\sqrt{2} &= 1 + (\sqrt{2} - 1) \\
\sqrt{2} &= 1 + \frac{1}{\sqrt{2} + 1} \\
\sqrt{2} + 1 &= 2 + (\sqrt{2} - 1) \\
\sqrt{2} &= 1 + \cfrac{1}{2 + \frac{1}{\sqrt{2} + 1}} \\
\sqrt{2} &= 1 + \cfrac{1}{2 + \frac{1}{2 + \frac{1}{2 + \cdots}}}
\end{aligned}$$

Then we obtain that $\sqrt{2} = [1, 2, 2, 2, \cdots] = [1, \overline{2}] = 1 + \cfrac{1}{2 + \frac{1}{2 + \frac{1}{2 + \cdots}}}$

Let K be the laurent-series field $k\left((x^{-1})\right)$. Define a function

$$\varphi : K - k[x] \to K, \qquad \varphi(\alpha) = 1/(\alpha - [\alpha])$$

where $[\alpha]$ is the polynomial part of α. For positive integers r let φ_r be the r-fold composition of φ with itself and let φ_0 be the identity map, namely,

$$\alpha_0 = \alpha, \quad \alpha_r = \varphi_r(\alpha), \quad \alpha_{r+1} = 1/(\alpha_r - [\alpha_r]) \qquad \text{for } r \geqslant 1.$$

In addition, $a_r := [\alpha_r]$ is called a **partial quotient of** α. Now, the continued fraction expansion of α is given by

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

One can write the latter continued fraction in short as $\alpha = [a_0, a_1, a_2, \ldots]$. The **convergents** of α are defined by setting $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$, and for $r \geqslant 0$,

$$q_r = a_r q_{r-1} + q_{r-2}, \quad p_r = a_r p_{r-1} + p_{r-2},$$

where $q_r, p_r \in k[x]$. We have the following equalities :

$$\begin{gathered}
p_r/q_r = [a_0; a_1, \ldots, a_r] \quad (r \geqslant 0), \\
q_r p_{r-1} - p_r q_{r-1} = (-1)^r \quad (r \geqslant -1), \\
\alpha = \frac{p_r \alpha_{r+1} + p_{r-1}}{q_r \alpha_{r+1} + q_{r-1}} = [a_0; a_1, \ldots, a_r, \alpha_{r+1}] \quad (r \geqslant -1), \\
\alpha_r = [a_r; a_{r+1}, \ldots] \quad (r \geqslant 0), \\
q_r/q_{r-1} = [a_r; a_{r-1}, \ldots, a_1] \quad (r \geqslant 1), \\
q_r \alpha - p_r = (-1)^r/(q_r \alpha_{r+1} + q_{r-1}) \quad (r \geqslant -1).
\end{gathered}$$

Example 2.8 *Given the polynomial* $f(x) = x^6 + 4x^5 + 4x^4 + 2x + 4$. *We want to find the continued fraction expansion of* $g(x) := \sqrt{f(x)}$. *The polynomial part of* $g(x)$ *is:*

$$a_0 = [\alpha_0] = x^3 + 2x^2$$

Then, the next term is:

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{g(x) - (x^3 + 2x^2)}$$

If we multiply and divide it by the conjugate we obtain the following equality:

$$\frac{1}{g(x)-(x^3+2x^2)}\cdot\frac{g(x)+\left(x^3+2x^2\right)}{g(x)+(x^3+2x^2)}=\frac{g(x)+\left(x^3+2x^2\right)}{g(x)^2-(x^3+2x^2)^2}=\frac{g(x)+x^3+2x^2}{2x+4}$$

Then we obtain that

$$a_1=[\alpha_1]=\left[\frac{g(x)+x^3+2x^2}{2x+4}\right]=\frac{2\left(x^3+2x^2\right)}{2x+4}=x^2$$

Similary, the next term is as follows:

$$\begin{aligned}\alpha_2=\frac{1}{\alpha_1-a_1}=\frac{1}{\frac{1}{g(x)-(x^3+2x^2)}-x^2}&=\frac{1}{\frac{g(x)+x^3+2x^2}{2x+4}-x^2}\\&=\frac{2x+4}{g(x)-(x^3+2x^2)}\cdot\frac{g(x)+\left(x^3+2x^2\right)}{g(x)+(x^3+2x^2)}\\&=\frac{(2x+4)\left(g(x)+x^3+2x^2\right)}{2x+4}\\&=g(x)+x^3+2x^2\end{aligned}$$

Then $a_2=[\alpha_2]=\left[g(x)+x^3+2x^2\right]=2x^3+4x^2=2(x^3+2x^2)=2a_0$. *Then we can stop at this point.*

We get the continued fraction expansion of $g(x)$ *as indicated below:*

$$\begin{aligned}\sqrt{f(x)}=g(x)=x^3+2x^2+&\cfrac{1}{x^2+\cfrac{1}{2\left(x^3+2x^2\right)+\cfrac{1}{x^2+\ddots}}}\\&=\left[x^3+2x^2,\overline{x^2,2\left(x^3+2x^2\right)}\right]=[a_0,\overline{a_1,2a_0}]\end{aligned}$$

Definition 9 *Let* a_i *be the* i*-th partial quotient of the continued fraction expansion of* $\sqrt{f(x)}$. *The continued fraction of* $\sqrt{f(x)}$ *is said to be* ***periodic*** *if there is a positive integer* n *such that* $a_{h+n}=a_h$ *for every* $h>1$, *the smallest such* n *is called the* ***period*** *of the continued fraction.*

Example 2.9 *In the example 2.8 the continued fraction expansion of* $g(x)$ *is periodic such that the period is* 2.

Theorem 2.11 *Let* C *be a hyperelliptic curve of genus* g *defined over the field* k

with $\mathrm{char}(k) \neq 0$ *by equation* $y^2 = f(x)$ *where* $f(x) \in k[x]$ *is of even degree* $2g+2$. *Assume that the leading coefficient of* $f(x)$ *is a square in* k. *Then if the continued fraction expansion of* $\sqrt{f(x)}$ *is periodic, it will be in the following form*

$$y = \sqrt{f(x)} = [a_0, \overline{a_1, \cdots, a_{n-1}, 2a_0}]$$

and it holds the followings:

- $a_{n-i} = a_i$ *for all* $i < n$.
- $\deg(a_i) < \deg(a_0)$ *for all* $i < n$.

The following properties can be found in [Adams & Razar (1980)] and [(Van der Poorten & Tran, 2000, Theorem 4.2)].

Theorem 2.12 *Let* $f(x) \in k[x]$ *is of even degree* $2g+2$, *for a number field* k. *Assume that the continued fraction expansion of* $\sqrt{f(x)}$ *is periodic. Then it is in the following form*

$$y = [a_0; \overline{a_1, a_2, \cdots, a_{m-1}, 2\gamma a_0, a_{m-1}, \cdots, a_2, a_1, 2a_0}]$$

where $a_{2(\frac{m-1}{2}-i)} = \gamma^{-1} a_{2i+1}$ *for any* $0 \leq i < \frac{m-1}{2}$, *for some* $\gamma \neq 0 \in k$.

Remark 2.1 *For the case* $\gamma = 1$ *we obtain* $n = m$. *But if* $\gamma \neq 1$ *then* $n = 2m$.

In the context of Theorem, we refer to the minimal value m as the **quasi-period length**. Therefore, when $\gamma = 1$, the period length is equal to the quasi-period length.

Lemma 2.1 *The continued fraction of* μy *is given by*

$$\mu y = \left[\mu a_0, \overline{a_1/\mu, \mu a_2, \ldots, \mu a_{m-1}, 2a_0/(k\mu), k\mu a_1, \ldots, a_{m-1}/(k\mu), 2a_0\mu}\right],$$

for any μ.

Remark 2.2 *In Theorem 2.12, if* $\gamma = 1$, *then the period is* m. *If* $k \neq 1$; *in particular,* m *is odd, then* μy *has the period length* m *if and only if* $\mu^2 = 1/k$.

Adams and Razar, [Adams & Razar (1980)] proved the following theorem for elliptic curves. These results were then extended to hyperelliptic curves. In the rest of this chapter, we will investigate the close relation between continued fraction expansion of $\sqrt{f(x)}$, where $f(x)$ is an even degree polynomial and the torsion order of the

divisor $D_\infty = [\infty_1 - \infty_2]$ on the Jacobian of the hyperelliptic curve $C : y^2 = f(x)$.

Theorem 2.13 (Adams & Razar (1980),Berry (1990)) *Let C be the hyperelliptic curve defined over k by the equation $y^2 = f(x)$ where $f(x) \in k[x]$ is of even degree $2g+2$, $g \geq 1$, that has no repeated root in $\overline{k}$, and the leading coefficient of $f(x)$ is a nonzero square in k. The divisor D_∞ is torsion if and only if the continued fraction of y is periodic.*

Corollary 2.1 *Assume that the curve $C : y^2 = f(x)$ satisfies the hypotheses in Theorem 2.13. Assume that the continued fraction of y is periodic. Then the continued fraction expansion of y is given by*

$$y = [a_0; \overline{a_1, a_2, \cdots, a_{m-1}, 2\gamma a_0, a_{m-1}, \cdots, a_2, a_1, 2a_0}]$$

where $a_{2(\frac{m-1}{2}-i)} = \gamma^{-1} a_{2i+1}$ for any $0 \leq i < \frac{m-1}{2}$, for some $\gamma \neq 0 \in k$.

Theorem 2.14 *Assume that the curve $C : y^2 = f(x)$ satisfies the hypotheses in Theorem 2.13. Then the order of the torsion divisor D_∞ is given by:*

$$\begin{aligned} |D_\infty| &= \sum_{i=0}^{m-1} \deg a_i \\ &= g + 1 + \sum_{i=1}^{m-1} \deg a_i \end{aligned}$$

Moreover, $\deg a_0 = g+1$, and $1 \leq \deg a_i \leq g$ for $1 \leq i \leq m-1$.

Corollary 2.2 *Assume that the curve $C := y^2 = f(x)$ satisfies the hypotheses in Theorem 2.13. Assume that the continued fraction of y is periodic with quasi-period length m. Then*

$$m + g \leq |D_\infty| \leq mg + 1$$

3. Construction of Curves Via Continued Fractions

3.1 Hyperelliptic Curves via Continued Fractions

The aim is to construct a 1-parameter family of hyperelliptic curves. We have seen some invariants of a hyperelliptic curve in the previous sections. Let C be a hyperelliptic curve defined over k by the equation $y^2 = f(x)$ where $f(x) \in k[x]$ is of even degree $2g+2$, $g \geq 1$, that has no repeated root in $\overline{k}$, and the leading coefficient of $f(x)$ is a nonzero square in k. Assume that the continued fraction expansion of y is periodic. Let us to fix the quasi-period length, m by starting from the smallest possible value 1. During this section assume that the order of the infinity divisor D_∞ is N and $a_i = a_i(x)$, which are the partial quotients of the continued fraction expansion of y for a given curve in the form $y^2 = f(x)$. We know also that

$$N = g + 1 + \sum_{i=1}^{m-1} \deg a_i$$

3.1.1 $m = 1$

First we assume that the quasi-period m of the continued fraction expansion of y is 1 then basicly, $y = [a_0, \overline{2a_0}]$ and $y^2 = {a_0}^2 + 1$. This implies that the order of the divisor D_∞ is just $g+1$, which is the degree of a_0.

3.1.2 $m = 2$

In this part we assume that the quasi-period m of the continued fraction of y is 2. Then $y = [a_0, \overline{a_1, 2a_0}]$, then $y^2 = \frac{2a_0}{a_1} + {a_0}^2$. One can say that the torsion order of the infinity divisor can be bounded as $2+g \leq N \leq 2g+1$, for genus g. We know that the hyperelliptic curve can be given by $y^2 = f(x)$ where $f(x)$ is a degree $2g+2$ polynomial. So $\frac{2a_0}{a_1}$ must be a polynomial. Moreover since the degree of a_0 is $g+1$ and the degree of a_1 is $N-g-1$. Then the degree of $\frac{2a_0}{a_1}$ is $2g+2-N$. Assume that $a_0 = x^{g+1} + \sum_{n=0}^{g} r_n x^n$ and $a_1 = \sum_{n=0}^{N-g-1} s_n x^n$. Looking at the degree, we can say that

$$\frac{2a_0}{a_1} = \frac{2}{s_{N-g-1}} x^{2g+2-N} + \sum_{n=0}^{2g+1-N} h^n x^n.$$

Consequently, we need to solve the equation $(\frac{2}{s_{N-g-1}} x^{2g+2-N} + \sum_{n=0}^{2g+1-N} h^n x^n) a_1 - 2a_0 = 0$ such that $s_{N-g-1} \neq 0$. The solution of this system gives us 1-parameter families of hyperelliptic curves. One of the explicit solution of this system can be given in the following theorem.

Theorem 3.1 *Let $\alpha > 1$ be any positive integer. For any $g > 2\alpha - 3$ there exists a 1-parameter family of hyperelliptic curves such that genus is g and the torsion order of the infinity divisor $D_\infty = \infty_1 - \infty_2$ of the Jacobian of the curve is $N = \alpha + g$. This family is given as follows:*

$$C : y^2 = \Big[x^{g+1} + \cdots + x^{g-\alpha+2} + (-1)^{\alpha-1}\left((t-1)^\alpha + (-1)^{\alpha-1}\right)\left(x^{g-\alpha+1} + x^{g-\alpha} + \cdots + x^{\alpha-1}\right)$$
$$+(-1)^{\alpha-1}\left(\sum_{i=2}^{\alpha}\left((t-1)^\alpha + (-1)^{\alpha-i}(t-1)^{i-1}\right)x^{\alpha-i}\right)\Big]^2 + \frac{1}{t}x^{g-\alpha+2} + x^{g-\alpha+1} + \cdots + x + 1$$

Proof. Since the period of the continued fraction of y is 2, $y^2 = \frac{2a_0}{a_1} + a_0^2$. Then by looking the equation of y^2, the square part is a_0 and the rest is $\dfrac{2a_0}{a_1}$. Then the degree of a_0 is $g+1$ and the degree of $\frac{2a_0}{a_1}$ is $g-\alpha+2$. Then $deg(a_1) = \alpha - 1$. We know that $N = deg(a_0) + deg(a_1)$, then $N = g + \alpha$. □

We can give 1 -parameter families of hyperelliptic curves such that quasi-period length m of y is 2 and genus is g, torsion order of the infinity divisors D_∞ is $N = k + g$ for some $k \in \mathbb{Z}$ and for some small genus g as follows:

1)$N = 2+g$ where $g > 2$:

$$C : y^2 = \left[x^{g+1} + x^g - \left(t^2 - 2t\right)\left(x^{g-1} + x^{g-2} + \cdots + x\right) - t^2 + t\right]^2 + \left(x^g + tx^{g-1} + \cdots + tx + t\right)/t$$

2) $N = 3+g$ where $g > 3$:

$$C : y^2 = [x^{g+1} + x^g + x^{g-1} + \left(t^3 - 3t^2 + 3t\right)\left(x^{g-2} + \cdots + x^2\right) + \left(t^3 - 3t^2 + 2t\right)x + t^3 - 2t^2 + t]^2 + \left(x^{g-1} + tx^{g-2} + \cdots + tx + t\right)/t$$

3) $N = 4+g$ where $g > 5$:

$$C : y^2 = [x^{g+1} + \ldots + x^{g-2} - \left(t^4 - 4t^3 + 6t^2 - 4t\right)\left(x^{g-3} + x^{g-4} + \cdots + x^3\right) - \left(t^4 - 4t^3 + 6t^2 - 3t\right)x^2 - t^4 + 3t^3 - 3t^2 + t]^2 + \left(x^{g-2} + tx^{g-3} + tx^{g-4} + \cdots + tx + t\right)/t$$

4) $N = 5+g$ where $g > 7$:

$$\begin{aligned} C : y^2 = &[x^{g+1} + x^g + \cdots + x^{g-3} + \left(t^5 - 5t^4 + 10t^3 - 10t^2 + 5t\right)\left(x^{g-4} + \ldots + x^4\right) \\ &+ \left(t^5 - 5t^4 + 10t^3 - 10t^2 + 4t\right)x^3 + \left(t^5 - 5t^4 + 10t^3 - 9t^2 + 3t\right)x^2 \\ &+ \left(t^5 - 5t^4 + 9t^3 - 7t^2 + 2t\right)x + t^5 - 4t^4 + 6t^3 - 4t^2 + t]^2 \\ &+ \left(x^{g-3} + tx^{g-4} + tx^{g-5} + \cdots + tx + t\right)/t \end{aligned}$$

Corollary 3.1 *There exists a one-parameter family of hyperelliptic curves defined on* $\mathbb{Q}$*, whose Jacobian has a rational point of order* 11 *and whose genus is either* 7 *or* 8*; order* 13 *and whose genus is either* 8, 9, 10 *or* 11*; order* 17 *and whose genus is either* 12, 13, 14 *or* 15*; order* 23 *and whose genus is either* 15, 16, 17, 18 *or* 19*.*

Example 3.1 $g = 7,\ N = 11$

$$C : y^2 = \left[x^8 + x^7 + x^6 + x^5 - \left(t^4 - 4t^3 + 6t^2 - 4t\right)\left(x^4 + x^3\right) - \left(t^4 - 4t^3 + 6t^2 - 3t\right)x^2 - t^4 + 3t^3 - 3t^2 + t\right]^2 + \left(x^5 + tx^4 + tx^3 + tx^2 + tx + t\right)/t$$

$g = 8,\ N = 11$

$$C : y^2 = \left[x^9 + x^8 + x^7 + \left(t^3 - 3t^2 + 3t\right)\left(x^6 + \cdots + x^2\right) + \left(t^3 - 3t^2 + 2t\right)x + t^3 - 2t^2 + t\right]^2 + \left(x^7 + tx^6 + \cdots + tx + t\right)/t$$

$g=8,\ N=13$

$$\begin{aligned} C: y^2 =& [x^9+x^8+\cdots+x^5+\left(t^5-5t^4+10t^3-10t^2+5t\right)\left(x^4\right) \\ &+\left(t^5-5t^4+10t^3-10t^2+4t\right)x^3+\left(t^5-5t^4+10t^3-9t^2+3t\right)x^2 \\ &+\left(t^5-5t^4+9t^3-7t^2+2t\right)x+t^5-4t^4+6t^3-4t^2+t]^2 \\ &+\left(x^5+tx^4+tx^3+tx^2+tx+t\right)/t \end{aligned}$$

Corollary 3.2 *Let g be an integer ≥ 1. For any integer N such that $2+g \leq N < \frac{3}{2}(g+1)$, there exists a one-parameter family of hyperelliptic curves defined over $\mathbb{Q}$ of genus g and whose Jacobian has a rational point of order N.*

In general, if $m=2$, then the period length and quasi-period length coincide yielding that $y=[a_0;\overline{a_1,2a_0}]$; or equivalently $y^2=a_0^2+\dfrac{2a_0}{a_1}$, where $a_0/a_1 \in k[x]$ is a polynomial whose degree is at most g. In fact, one may assume that $a_0=a_1h(x)$, $h(x)\in k[x]$, and $\deg a_1+\deg h=g+1$. It follows that to maximize the order of the torsion divisor at infinity $\deg a_1$ must be g; and hence $h(x)$ is a linear polynomial.

Theorem 3.2 *Fix an integer $g\geq 1$. Let α be an integer such that $1\leq\alpha\leq g$. Let $h(x), a_1(x)\in k[x]$ be polynomials of degree α and $g+1-\alpha$ respectively. Assume that the polynomials $h(x)$ and $a_1(x)^2h(x)+2$ have no repeated roots.*

Set C to be the hyperelliptic curve defined over k by the equation

$$y^2=h(x)\left(a_1(x)^2h(x)+2\right).$$

Then the divisor at infinity on C is torsion of order $2g+2-\alpha$. Moreover, $y=[a_1(x)h(x);\overline{a_1(x),2a_1(x)h(x)}]$.

Corollary 3.3 *Fix an integer $g\geq 1$. Let $h(x)\in k[x]$ be of degree α, $1\leq\alpha\leq g$. Let C be the hyperelliptic curve $y^2=h(x)\left(x^{2(g+1-\alpha)}h(x)+2\right)$. The divisor at infinity is torsion of order $2g+2-\alpha$. In particular, given an integer N, $g+2\leq N\leq 2g+1$, there exists a hyperelliptic curve C of genus g whose Jacobian has a k-rational point of order N.*

Example 3.2 $g=5,\ N=11$

$$\begin{aligned} \text{Take } h(x) =& x+1,\ a_1(x)=x^5+1 \\ C: y^2 =& (x+1)\left((x^5+1)^2(x+1)+2\right) \end{aligned}$$

$g=6,\ N=13$

$$\begin{aligned} \text{Take } h(x) =& x+1,\ a_1(x)=x^6+1 \\ C: y^2 =& (x+1)\left((x^6+1)^2(x+1)+2\right) \end{aligned}$$

3.1.3 $m = 3$

We can use similar idea to construct 1-parameter hyperelliptic curves such that the quasi-period length of the continued fraction of y is 3. The continued fraction expansion is given as

$$y = \left[a_0, \overline{a_1, \frac{a_1}{\gamma}, 2\gamma a_0, \frac{a_1}{\gamma}, a_1, 2a_0}\right]$$

where γ is a skew-value. Then we obtain

$$y^2 = a_0^2 + \frac{2a_0a_1 + 1}{a_1^2 + \gamma}$$

By using similar idea with the case $m = 2$, the rational part must be a polnomial, with the leading coefficient is $\frac{2a_0}{a_1}$ and the degree is $\deg(a_0) - \deg(a_1)$. In this case the order of the infinity divisor is given as follows:

$$\begin{aligned} N = \sum_{i=0}^{2} \deg a_i &= \deg a_0 + \deg a_1 + \deg a_2 \\ &= 2\deg a_1 + \deg a_0 \\ &= 2\deg a_1 + g + 1. \end{aligned}$$

The following theorem provide us a solution:

Theorem 3.3 *Let g be an even (respectively odd) integer > 1. For any odd (resp. even) integer N such that $3 + g \leq N \leq 2g + 1$ there exists a 1 -parameter family of hyperelliptic curves defined over $\mathbb{Q}$ of genus g and whose Jacobian has a rational point of order N.*

The following curves is a family of the hyperelliptic curves with genus $g > 1$, torsion order $N = 2r + g + 1, \forall r \leqslant \frac{g}{2}$

$$y^2 = \left(\frac{1}{2}\left(2a^2x^{g+1} + a^3x^r + 2x^{g-2r+1}\right)/a^2\right)^2 + \left(2x^{g-r+1} + a\right)/a$$

where $r = \deg(a_1)$.

Proof. By looking the continued fraction of y

$$y^2 = {a_0}^2 + \frac{2a_0a_1 + 1}{{a_1}^2 + \gamma}.$$

Then in the given equality the square part represents a_0, so $\deg a_0 - \deg a_1 = g - r + 1$. Then $\deg a_1 = r$ and $N = 2r + g + 1$. □

In general we obtain the following: we have to consider $m = 3$ in two subcases:

i) when the period length $n = m$, and ii) when the period length $n = 2m$. In the first case $y = [a_0; \overline{a_1, a_1, 2a_0}]$, whereas in ii) $y = [a_0; \overline{a_1, \gamma^{-1}a_1, 2\gamma a_0, \gamma^{-1}a_1, a_1, 2a_0}]$. In either cases $y^2 = a_0^2 + \dfrac{2a_0a_1 + 1}{a_1^2 + \gamma}$, where γ is taken to be 1 in i).

Theorem 3.4 *Fix an integer $g \geq 1$. Let α be an integer such that $1 \leq \alpha \leq \lfloor (g+1)/2 \rfloor$. Let $a_1(x), q(x) \in k[x]$ be polynomials of degree α and $g+1-2\alpha$ respectively. Set C to be the hyperelliptic curve defined over k by the equation*

$$y^2 = \Big(\gamma q(x)a_1(x)^2 + a_1(x) + \gamma^2 q(x)\Big)^2 + 4\gamma^2 q(x)a_1(x) + 4\gamma.$$

Then the divisor at infinity on C is torsion of order $g+1+2\alpha$. Moreover,

$$y = [\gamma q(x)a_1(x)^2 + a_1(x) + \gamma^2 q(x); \overline{a_1(x), \gamma^{-1}a_1(x), 2\gamma a_0(x), \gamma^{-1}a_1(x), a_1(x), 2a_0(x)}].$$

Proof. Since $y^2 = a_0^2 + \dfrac{2a_0a_1 + 1}{a_1^2 + \gamma}$, where $\gamma = 1$ if $m = n$, one may assume that $a_0(x) = \dfrac{h(x)(a_1(x)^2 + \gamma) - 1}{2a_1(x)}$ for some $h(x) \in k[x]$ where $\deg h + \deg a_1 = g + 1$ and $\deg h > \deg a_1$. One may then write $h(x) = q(x)a_1(x) + 1/\gamma$ for some non-constant polynomial $q(x) \in k[x]$. In particular, $2\deg a_1 + \deg q = g + 1$. □

Corollary 3.4 *Fix an integer $g \geq 1$. Let $h(x) \in k[x]$ be of degree α, $1 \leq \alpha \leq \lfloor (g+1)/2 \rfloor$. Let C be the hyperelliptic curve $y^2 = \Big(\gamma x^{g+1-2\alpha}h(x)^2 + h(x) + \gamma^2 x^{g+1-2\alpha}\Big)^2 + 4\gamma^2 x^{g+1-2\alpha}h(x) + 4\gamma$. The divisor at infinity is torsion of order $g+1+2\alpha$. In particular, given an integer N, $g+3 \leq N \leq g+1+2\lfloor (g+1)/2 \rfloor$, there exists a hyperelliptic curve C of genus g whose Jacobian has a k-rational point of order N.*

3.1.4 $m = 4$

In this case the continued fraction expansion of y is periodic with period $m = 4$, so $y = [a_0, \overline{a_1, a_2, a_1, 2a_0}]$. Hence

$$y^2 = \frac{2a_0a_1a_2 + {a_0}^2{a_1}^2a_2 + 2{a_0}^2a_1 + 2a_0 + a_2}{2a_1 + {a_1}^2a_2} = a_0^2 + \frac{2a_0a_1a_2 + 2a_0 + a_2}{2a_1 + {a_1}^2a_2} \tag{3.1}$$

By using similar idea with the case $m = 2$, the rational part must be a polnomial, with the leading coefficient is $\frac{2}{a_1}$ and the degree is $\deg(a_0) - \deg(a_1)$. In this case

the order of the infinity divisor is given as follows:

$$N = \sum_{i=0}^{2} \deg a_i = \deg a_0 + 2\deg a_1 + \deg a_2$$
$$= 2\deg a_1 + \deg a_2 + g + 1.$$

An example of a solution of this case is given as follows:

Example 3.3 *Let $g > 1$ be an integer. For any N such that $4+g \leq N \leq \frac{5}{2}g+2$ there exists a 1-parameter family of hyperelliptic curves of genus g such that the order of the infinity divisor is* N.

In the following lists we are giving the 1-parameter family of genus g hyperelliptic curves such that the order of their infinity divisor is N. We are categorizing our curves by N or g is some cases.

Let $4 \leq k \leq g+2$ be an integer where g is the genus of the curves. Let $N = k+g$, $\left\lceil \frac{g}{k-2} \right\rceil = m, \left\lceil \frac{g-(k-4)}{k-2} \right\rceil = n$.

$$y^2 = \left(-\frac{1}{2} \sum_{i=1}^{m-1} \left((-t)^i x^{(k-2)(i-1)+1} \right) + \frac{1}{2}(-t)^m x^{(k-2)(m-1)+1} \right.$$
$$\left. -\frac{1}{2} \sum_{i=1}^{n-1} \left((-t)^{i-1} x^{(k-2)i-1} \right) + \frac{1}{2}(-t)^{n-1} x^{(k-2)\cdot n-1} + x^{g+1} + \frac{2}{t} x^{g-(k-3)} + \frac{t}{2} x \right)^2$$
$$+1 + \frac{2}{t} x^g + \frac{2}{t^2} x^{g-(k-2)} - t^{n-2}(-x)^{(k-2)n-2} - t^{(m-1)}(-x)^{(k-2)(m-1)}$$

Let $N = 2g+3$.

Respectively for $g = 2,\ 3$ and 4 the curves are given as follows:

$$y^2 = \left(x^3 + \frac{x^2}{2}\left(\frac{4}{t}+5\right) + \frac{x}{2}\left(\frac{5}{t}+\frac{2}{t^2}+2\right) + \frac{2}{t} \right)^2 + \frac{2x^2}{t} + \left(\frac{5}{t}+\frac{2}{t^2}\right)x + \frac{2}{t}$$

$$y^2 = \left(x^4 + \frac{x^3}{2}\left(\frac{2}{t}+3\right) + \frac{x^2}{2}\left(\frac{4}{t}-\frac{2}{t^2}+5\right) + \frac{x}{2}\left(\frac{5}{t}+\frac{1}{t^2}-\frac{2}{t^3}+2\right) \right)^2 + \frac{2x^3}{t}$$
$$+ \left(\frac{5}{t}+\frac{1}{t^2}-\frac{2}{t^3}\right)x + \frac{3x^2}{t} + \frac{2}{t}$$

$$y^2 = \left(x^5 + \frac{t}{2}x^2 - \frac{2x^4}{t^3} + \frac{x}{t^2}\right)^2 + \frac{2x^3}{t} - \frac{4x^2}{t^4} + 1$$

For $g \geq 5$ the curves are given as follows:

$$y^2 = \left(x^{g+1} + \frac{t}{2}x^{g-2} + x^5 + \frac{t}{2}x^2 - \frac{2x^4}{t^3} + \frac{x}{t^2}\right)^2 + \frac{2x^{g-1}}{t} + x^{g-4} + \frac{2x^3}{t} - \frac{4x^2}{t^4} + 1$$

Let $N = 2g + k$ where $4 \leq k \leq \dfrac{g+4}{2}$ is an integer. In this case the curves are given as follows: .

$$\begin{aligned} y^2 = &\left(x^{g+1} + \frac{t}{2}x^{g-k+3} + x^{2(k-2)}\left(1 + \frac{4}{t^4}\right) + \frac{t}{2}x^{k-2} + \frac{1}{t^2}\right)^2 + \frac{2x^{g-k+3}}{t} \\ &+ x^{g-2k+5} + \frac{2x^{k-2}}{t}\left(1 + \frac{4}{t^4}\right) + 1 \end{aligned}$$

In general, we obtain the following:

We now consider the case where $m = 4$, and hence the quasi-period length and the period length are the same. One has $y = [a_0; \overline{a_1, a_2, a_1, 2a_0}]$.

Theorem 3.5 *Fix an integer $g \geq 1$. Let α, β be integers such that $2 \leq \alpha + \beta \leq g+1$. Let $a_1(x), a_2(x) \in k[x]$ be non-constant polynomials of degree α, β, respectively. There exists $r(x) \in [x]$ of degree at most $\beta - 1$ such that the Weierstrass equation*

$$y^2 = \frac{1}{4}\left(qa_1a_2 + ra_1 + q\right)^2 + qa_2 + r \tag{3.2}$$

where $q(x) = r(x)a_1(x) - a_2(x)$, $\deg q = g + 1 - \alpha - \beta$, describes a hyperelliptic curve C for which the divisor at infinity on C is torsion of order $g + 1 + 2\alpha + \beta$.

Proof. Given that the continued fraction expansion of y has period length 4, one sees that

$$y^2 = a_0^2 + \frac{2a_0a_1a_2 + 2a_0 + a_2}{2a_1 + a_1^2a_2}.$$

Now for the last equation to be Weierstrass, one may assume the existence of $h(x) \in k[x]$, $\deg h \leq g$, such that $h(2a_1 + a_1^2a_2) = 2a_0a_1a_2 + 2a_0 + a_2$. In other words, one may write

$$a_0 = \frac{h(2a_1 + a_1^2a_2) - a_2}{2(a_2a_1 + 1)} = \frac{ha_1}{2} + \frac{ha_1 - a_2}{2(a_1a_2 + 1)}.$$

Now we find conditions under which $a_0 \in k[x]$. One notices that $\deg h + \deg a_1 = g + 1$, moreover, $\deg h \geq \deg a_2$; or $h = qa_2 + r$ where $0 \leq \deg q \leq g - 1$ and $0 \leq \deg r < \deg a_2$.

This shows that

$$a_0 = \frac{ha_1+q}{2} + \frac{ra_1-a_2-q}{2(a_1a_2+1)}.$$

In particular, the Weierstrass equation becomes

$$y^2 = \frac{1}{4}\left(qa_1a_2+ra_1+q\right)^2 + qa_2 + r, \text{ where } ra_1 - a_2 + q = 0.$$

□

Example 3.4 *In equation (3.3) of Theorem 3.5, if we set $a_2 = ra_1 - q$, hence $h = rqa_1 - q^2 + r$, we obtain the Weierstrass equation*

$$y^2 = \frac{1}{4}\left(rqa_1^2 - q^2a_1 + ra_1 + q\right)^2 + rqa_1 - q^2 + r.$$

Choosing r, q to be k-rationals when g is odd; and q to be k-rational whereas r to be linear if g is even, the order of the torsion divisor at infinity becomes $5(g+1)/2$ if g is odd; and $5g/2+2$ if g is even.

3.1.5 $m = 5$

In what follows we investigate the quasi-period length $m = 5$. The continued fraction expansion of y is given by $[a_0; \overline{a_1, a_2, \gamma a_2, a_1/\gamma, 2\gamma a_0, a_1/\gamma, \gamma a_2, a_2, a_1, 2a_0}]$. This yields that

$$y^2 = a_0^2 + \frac{1+\gamma a_2^2 + 2a_0(a_1+\gamma a_2+\gamma a_1 a_2^2)}{\gamma + 2\gamma a_1 a_2 + a_1^2(1+\gamma a_2^2)}$$

Theorem 3.6 *Fix an integer $g \geq 1$. Let α, β be non-zero integers such that $\beta \leq \alpha \leq 2\beta$ and . Let $a_1(x)$ be of degree α. Let $t(x) \in [x]$ be of degree $2\beta - \alpha$. Then there exists $a_2(x) \in k[x]$ of degree β and $r(x) \in k[x]$ of degree at most $\beta - 1$ such that the Weierstrass equation*

$$\begin{aligned} y^2 &= \frac{1}{4}\left(\left(-\gamma t(x) + \gamma a_2(x) r(x)\right)\left(a_1(x)a_2(x)+1\right) + a_1(x)r(x)\right)^2 \\ &+ a_2(x)\left(-\gamma t(x) + \gamma a_2(x) r(x)\right) + r(x) \end{aligned}$$

describes a hyperelliptic curve C over k for which the divisor at infinity has order $g+1+2\alpha+2\beta$.

Proof. Setting the non-square part to be a polynomial $h(x)$ of degree at most g, one

gets

$$a_0(x) = \frac{-1 + ha_1^2 - \gamma a_2^2 + h\gamma + 2a_1a_2h\gamma + a_1^2a_2^2\gamma h}{2(a_1 + a_2\gamma + \gamma a_1a_2^2)} = \frac{a_1h}{2} + \frac{-1 - \gamma a_2^2 + h\gamma + a_1a_2h\gamma}{2(a_1 + a_2\gamma + \gamma a_1a_2^2)}.$$

Setting $h = qa_2 + r$ with $\deg r < \deg a_2$, one has

$$a_0 = \frac{a_1h + q}{2} + \frac{-1 - \gamma a_2^2 - qa_1 + r\gamma + a_1a_2r\gamma}{2(a_1 + a_2\gamma + \gamma a_1a_2^2)}.$$

Let $t(x) \in [x]$ be such that $\deg t + \deg a_1 = 2\beta$, $\beta \geq 1$. Now there is $a_2(x) \in [x]$ of degree β such that $t(x)a_1(x) = a_2(x)^2 + f(x)$ where $\deg f < \beta$. Set $r(x) = -f(x) + 1/\gamma$ and $q(x) = -\gamma t(x) + \gamma a_2(x)r(x)$. The Weierstrass equation describing C becomes

$$\begin{aligned} y^2 &= \frac{1}{4}\left((-\gamma t(x) + \gamma a_2(x)r(x))\left(a_1(x)a_2(x) + 1\right) + a_1(x)r(x)\right)^2 \\ &+ a_2(x)\left(-\gamma t(x) + \gamma a_2(x)r(x)\right) + r(x) \end{aligned}$$

□

If $\deg q < 2\deg a_2$, then $-1 - \gamma a_2^2 - qa_1 + r\gamma + a_1a_2r\gamma = 0$. We now use the assumption that $a_1 = ta_2$ for some $t \in [x]$ of degree at least 0. This directly implies that $r = 1/\gamma$. It follows that $ta_2 - qt - \gamma a_2 = 0$, whence $a_2 = ta_2'$ and $q = (t - \gamma)a_2'$. In particular, $\deg q = \deg a_1 < 2\deg a_2$. The curve is now described by

$$\begin{aligned} y^2 &= \frac{1}{4}\left(a_1(qa_2 + r) + q\right)^2 + qa_2 + r \\ &= \frac{a_2'^2}{4}\left((t - \gamma)\left(t^3a_2'^2 + 1\right) + t^2/\gamma\right)^2 + t(t - \gamma)a_2'^2 + 1/\gamma. \end{aligned}$$

If $\deg q \geq 2\deg a_2$, then using the assumption that $a_1 = ta_2$ for some $t \in [x]$, one has again that $r = 1/\gamma$. There is $u \in [x]$ such that

$$-\gamma a_2 - qt + ta_2 = 2u(t + \gamma + \gamma ta_2^2).$$

Now the choice $q = -2\gamma a_2^2u$ yields that $(t - \gamma)a_2 = 2u(t + \gamma)$. Picking $a_2 = 2(t + \gamma)a_2'$ gives that $u = (t - \gamma)a_2'$ and the Weierstrass equation becomes

$$y^2 = \frac{1}{4}\left(2t(t + \gamma)a_2'\left(-16\gamma(t - \gamma)(t + \gamma)^3a_2'^4 + 1/\gamma\right) - 8\gamma(t - \gamma)(t + \gamma)^2a_2'^3\right)^2 + (t - \gamma)a_2'.$$

3.1.6 $m = 6$

Fixing an integer $m \geq 0$, we set $\mathbb{Q}(\mathbf{w}) := \mathbb{Q}(w_1, \cdots, w_m)$, where $w_1, \cdots, w_m$ are algebraically independent. In this section, we construct hyperelliptic curves C of genus g over $\mathbb{Q}(\mathbf{w})$ described by the equation

$$y^2 = h_{2g+2}(\mathbf{w})^2 x^{2g+2} + h_{2g+1}(\mathbf{w}) x^{2g+1} + \cdots + h_0(\mathbf{w}), \qquad h_i(\mathbf{w}) \in \mathbb{Q}(\mathbf{w}), \quad i = 0, \cdots, 2g+2.$$

The curve C admits two $\mathbb{Q}(\mathbf{w})$-rational points at infinity denoted by ∞_1 and ∞_2.

We investigate the case when the divisor $D_\infty = \infty_1 - \infty_2$ in the Jacobian of C is torsion with the quasi-period length m is the same as period length n and both are equal to 6. This means that the continued fraction expansion of y is given by

$$[a_0(x); \overline{a_1(x), a_2(x), a_3(x), a_2(x), a_1(x), 2a_0(x)}] \tag{3.3}$$

where $\deg a_0 = g+1$ and $1 \leq \deg a_i \leq g$ when $i = 1, 2, 3$.

In order to construct our desired curves, a solution of a certain polynomial Diophantine equation must be found.

Lemma 3.1 *Let $r(x), q(x), a_1(x), a_2(x), a_3(x) \in \mathbb{Q}[x]$. The polynomial Diophantine equation*

- $2q(x) - 2a_2(x) + a_1(x)r(x) + a_3(x)r(x) - 2q(x)a_1(x)a_2(x) + a_1(x)a_2(x)a_3(x)r(x)$
- $a_2(x)^2 a_3(x) \equiv 0$

has the following solution

$$\begin{aligned} q(x) &= u(x)r(x)/2, \\ a_2(x) &= a_1(x)r(x), \\ a_3(x) &= a_1(x)^2 u(x) r(x) + a_1(x) + u(x), \end{aligned}$$

where $u(x) \in \mathbb{Q}[x]$.

Proof. One may check that the claimed solution satisfies the polynomial Diophantine equation. □

Theorem 3.7 *Fix an integer $g \geq 3$. Let $\alpha, \beta \geq 1, \gamma \geq 0$ be integers such that $2\alpha + 2\beta + \gamma = g + 1$. Let $a_1(x), r(x), u(x) \in \mathbb{Q}[x]$ be of degrees α, β, γ, respectively. If the*

affine equation

$$y^2 = r(x)^2\left(u(x)(a_1(x)^2r(x)+1)+a_1(x)\right)^2+4\left(u(x)a_1(x)r^2(x)+r(x)\right)$$

describes a hyperelliptic curve C, then the divisor at infinity is torsion of order $g+1+6\alpha+3\beta+\gamma$.

In addition, if $\beta=1$, and the Galois group of the polynomial

$$r(x)\left(u(x)(a_1(x)^2r(x)+1)+a_1(x)\right)^2+4\left(u(x)a_1(x)r(x)+1\right)$$

is either the full symmetric group $\boldsymbol{S}_{2g+1}$ or the alternating group $\boldsymbol{A}_{2g+1}$, then the Jacobian J_C of C satisfies that $\mathrm{End}(J_C)=$*, in particular, J_C is an absolutely simple abelian variety*

Proof. In view of (3.3), a hyperelliptic curve C for which the divisor at infinity is torsion with $m=n=6$ is described by an equation of the form

$$y^2 = a_0^2+\frac{a_2(2+a_2a_3)+2a_0(1+a_2a_3+a_1a_2(2+a_2a_3))}{(1+a_1a_2)(a_3+a_1(2+a_2a_3))}.$$

In order for the latter equation to be a polynomial equation, the latter fraction must be a polynomial $h\in\mathbb{Q}[x]$. This yields that

$$a_0=\frac{a_1h}{2}+\frac{-a_2^2a_3+(a_1+a_3)h+a_2(-2+a_1a_3h)}{2(1+a_2a_3+a_1a_2(2+a_2a_3))}.$$

By comparing the degrees of the numerator and denominator of the latter fraction as polynomials in a_1,a_2 and a_3, we may assume that $h=2qa_2+r$ with $\deg r<\deg q$ to obtain that

$$a_0=\frac{a_1h+2q}{2}+\frac{-2a_2-2q+a_1r+a_3r-2qa_1a_2+a_1a_2a_3r-a_2^2a_3}{2(1+a_2a_3+a_1a_2(2+a_2a_3))}.$$

We notice that if the degree of $q(x)$ is strictly less than the sum of the degrees of $a_2(x)$ and $a_3(x)$, then the numerator of the latter fraction is of strictly less degree than the denominator. Therefore, for a_0 to be a polynomial in $\mathbb{Q}[x]$, we may assume that $-2a_2-2q+a_1r+a_3r-2qa_1a_2+a_1a_2a_3r-a_2^2a_3\equiv 0\in\mathbb{Q}[x]$. According to Lemma 3.1, a solution to this polynomial Diophantine equation is provided giving rise to the affine equation $y^2=(a_1h+2q)^2/4+h$. After using the explicit description of the solution in Lemma 3.1, the curve C is described by

$$y^2 = r(x)^2\left(u(x)(a_1(x)^2r(x)+1)+a_1(x)\right)^2+4\left(u(x)a_1(x)r^2(x)+r(x)\right).$$

Now, when $\beta = 1$, the rest of the statement will follow from [(Zarhin, 1999, Theorem 1.3)]. □

Remark 3.1 *In Theorem 4.1, we insist that* $\beta := \deg r \geq 1$, *since otherwise* $a_3 = 2a_0$. *This means that in (3.3), the quasi period length,* m, *and the period length,* n, *satisfy that* $m = n = 3$.

We notice that in Theorem 4.1, if $a_1(x) = \sum_{i=0}^{\alpha} A_i x^i$, $r(x) = \sum_{i=1}^{\beta} R_i x^i$, and $u(x) = \sum_{i=0}^{\gamma} U_i x^i$, then the curve C is defined by an equation of the form $y^2 = f(x)$ where

$$f(x) \in \mathbb{Q}[A_0, \cdots A_\alpha, R_0, \cdots R_\beta, U_0, \cdots, U_\gamma][x].$$

The discriminant of C is a constant multiple of the discriminant Δ_f of the polynomial f, see for example [Lockhart (1994)] or [Liu (1996)], hence it is a polynomial in $\mathbb{Q}[A_0, \cdots A_\alpha, R_0, \cdots R_\beta, U_0, \cdots, U_\gamma]$. If we consider the affine space $\mathbb{A}^{\alpha+\beta+\gamma+3}$ with coordinates $A_0, \cdots A_\alpha$, $R_0, \cdots R_\beta$, $U_0, \cdots, U_\gamma$, then for a choice $(A_0, \cdots A_\alpha, R_0, \cdots R_\beta, U_0, \cdots, U_\gamma) \in \mathbb{A}^{\alpha+\beta+\gamma+3}$, the equation $y^2 = f(x)$ defines a hyperelliptic curve of genus g over $\mathbb{Q}$ if and only if $(A_0, \cdots A_\alpha, R_0, \cdots R_\beta, U_0, \cdots, U_\gamma)$ is chosen to lie in the complement of the hypersurface $\Delta_f = 0$ in the affine space $\mathbb{A}^{\alpha+\beta+\gamma+3}$.

As a direct consequence of Theorem 4.1, we get the following result.

Corollary 3.5 *Fix an integer* $g \geq 3$. *Let* N *be an integer such that* $3g \leq N \leq 4g+1$. *If there exists integers* $\alpha, \beta \geq 1, \gamma \geq 0$ *such that* $2\alpha + 2\beta + \gamma = g + 1$ *and* $N = g + 1 + 6\alpha + 3\beta + \gamma$, *then there exists infinitely many hyperelliptic curves of genus* g *over* $\mathbb{Q}$ *whose Jacobian posses a rational point of order* N. *In particular, if* g *is odd, respectively even, there are infinitely many hyperelliptic curves of genus* g *over* $\mathbb{Q}$ *whose Jacobian posses a rational point of order* $4g+1$, *respectively* $4g-1$.

Although our trials to study hyperelliptic curves C for which the corresponding continued fraction has quasi-period length $m \leq 5$ yielded torsion divisors at infinity with order $\mathrm{O}(kg)$, where $k < 3$, we successfully obtained families of hyperelliptic curves whose jacobain contains torsion points whose order is not listed in literature. As an example, when $m = n = 4$, one obtains the following equation

$$y^2 = \left(rqa_1^2 - q^2 a_1 + ra_1 + q\right)^2 + 4(rqa_1 - q^2 + r).$$

Choosing r, q to be $\mathbb{Q}$-rationals and $q^2 \neq r$ when g is odd; and q to be $\mathbb{Q}$-rational whereas r to be a linear polynomial if g is even, the order of the torsion divisor at

infinity becomes $5(g+1)/2$ if g is odd; and $5g/2+2$ if g is even.

As a result, we can summarize all of the small quasi-period lengths from one to six and the order of the infinity divisor as follows:

Quasi period of continued fraction expansion of $\sqrt{f(x)} := m$	**Torsion Order of $D_\infty := N$**
$\mathbf{m=1}$	$\mathbf{N=g+1}$
$\mathbf{m=2}$	$\mathbf{g+2 \leq N \leq 2g+1}$
$\mathbf{m=3}$	$\mathbf{g+2 \leq N \leq 2g}$
$\mathbf{m=4}$	**If g is odd:** $\mathbf{N \leq \frac{5g+5}{2}}$ **If g is even:** $\mathbf{N \leq \frac{5g+4}{2}}$
$\mathbf{m=5}$	$\mathbf{N \leq 3g+3}$
$\mathbf{m=6}$	**If g is odd:** $\mathbf{N \leq 4g+1}$ **If g is even:** $\mathbf{N \leq 4g-1}$

Example 3.5 *Consider the following family of hyperelliptic curves of genus* 3

$$C_t : y^2 = (2(x^2+t)^2+(x^2+t)+1)^2+4(2(x^2+t)+1)$$

over $\mathbb{Q}(t)$*. Since the discriminant of* C_t *is given by* $2^{48}\cdot 5^4\cdot(1+t)(5+5t+4t^3)$*, if* $t \neq -1$*, then the class of the divisor* $(1:2:0)-(1:-2:0)$ *on the Jacobian of* C_t *is of order* 10*.*

3.2 Explicit families

In this section we provide explicit parametric families of hyperelliptic curves of genus $g \geq 3$ whose Jacobian possess $\mathbb{Q}$-rational torsion points of orders that does not appear in the literature.

Theorem 3.8 *There exists infinitely many hyperelliptic curves of genus* 3 *over* $\mathbb{Q}$

whose Jacobians posses a rational point of order 13.

Proof. In Theorem 4.1, pick $r(x) = ax + b$, $a \neq 0$, to be a linear polynomial in $\mathbb{Q}[x]$, $u(x) = u \in \mathbb{Q} \setminus \{0\}$, and $a_1(x) = cx + d \in \mathbb{Q}[x]$, $c \neq 0$. When the discriminant of this curve is nonzero, we get a 5-parametric family of hyperelliptic curves satisfying the hypothesis of the theorem, where that divisor at infinity is $(1 : a^2 \cdot c^2 \cdot u : 0) - (1 : -a^2 \cdot c^2 \cdot u : 0)$. □

In a similar fashion, one may prove the following theorem.

Theorem 3.9 *There exists infinitely many hyperelliptic curves of genus* 4 *over* $\mathbb{Q}$ *whose Jacobians posses a rational point of order* 15.

Example 3.6 *If* $u \neq 0$, *then the hyperelliptic curve* $C^{13}_{u,t}$ *of genus* 3 *described by the equation*

$$y^2 = (x+t)^2(2t+u+x+u(x+t)(x+2t)^2)^2 + 4(t+x+u(x+t)^2(x+2t))$$

satisfies that the divisor at infinity is torsion of order 13.

Example 3.7 *Consider the genus* 4 *hyperelliptic curve described by*

$$C^{15}_{s,t} : y^2 = (x+t)^2\left(x+(x-s)(1+x^2(x+t))\right)^2 + 4\left(t+x+x(-s+x)(t+x)^2\right).$$

For a choice of s,t *such that the discriminant of* $C_{s,t}$ *is nonzero, one sees that the divisor at infinity* $(1:1:0) - (1:-1:0)$ *is torsion of order* 15.

Remark 3.2 *In examples 3.6, the equation describing the curve* $C^{13}_{u,t}$ *is of the form* $(x+t)f_{u,t}(x)$ *where the polynomial* $f_{u,t}$ *has generic Galois group* $\boldsymbol{S}_7$. *The latter statement can be justified by seeing that the specialization* $f_{1,1}$ *has Galois group* $\boldsymbol{S}_7$. *It follows that* $f_{u,t}$ *has Galois group* $\boldsymbol{S}_7$ *for infinitely many pairs* u,t. *According to Theorem 4.1, this means that the Jacobian* $J_{C^{13}_{u,t}}$ *of* $C^{13}_{u,t}$ *satisfies that* $\mathrm{End}(J_{C^{13}_{u,t}}) =$ *and that* $J_{C^{13}_{u,t}}$ *is an absolutely simple abelian variety for infinitely many values of* u,t.

The same argument yields that the Jacobian of $C^{15}_{s,t}$ *in Example 3.7 is an absolutely simple variety for infinitely many choices of* s,t.

We notice that for $g \geq 5$, there are at least two integers N in the interval $[3g, 4g+1]$ when g is odd, $[3g, 4g-1]$ when g is even, satisfying the hypotheses of Corollary 3.5.

Example 3.8 *Consider the following families of hyperelliptic curves of genus* 5

$$\begin{aligned} C^{17}_{s,t} &: y^2 = 4(t+x+x(t+x)^2(x^2+s)) + (x+t)^2(x+(x^2+s)(1+x^2(x+t)))^2 \\ C^{18}_{s,t,u} &: y^2 = (x^2+s)^2(t+u+x+u(x+t)^2(x^2+s))^2 + 4(s+x^2+u(x+t)(x^2+s)^2) \\ C^{21}_{s,t,u} &: y^2 = 4(s+x+u(x+s)^2(x^2+t)) + (x+s)^2(t+u+x^2+u(x+s)(x^2+t)^2)^2 \end{aligned}$$

corresponding to the triple $(\alpha,\beta,\gamma) = (1,1,2),(2,1,0),(1,2,0)$*, respectively, in Theorem 4.1. In fact, for the triple* $(1,1,2)$*, we chose* $a_1(x) = x$*,* $r(x) = x+t$*,* $u(x) = x^2+s$*, which implies that the divisor at infinity is torsion of order* 17*.*

For the triple $(1,2,0)$*, we chose* $a_1(x) = x+t$*,* $r(x) = x^2+s$*,* $u(x) = u \in \mathbb{Q}\setminus\{0\}$*, yielding that the divisor at infinity is torsion of order* 18*. Finally, for the triple* $(2,1,0)$*, we chose* $a_1(x) = x^2+t$*,* $r(x) = x+s$*,* $u(x) = u \in \mathbb{Q}\setminus\{0\}$*, with the divisor at infinity being torsion of order* 21*.*

The same argument as in Remark 3.2 shows that the Jacobians of the curves $C^{17}_{s,t}$ *and* $C^{21}_{s,t,u}$ *are absolutely simple varieties for infinitely many choices of* s,t,u*.*

4. Quadratic Torsion Order

In this chapter we will explain a different method to construct hyperelliptic curves. Constructing a quadratic torsion order begins with the works of Leprévost and Flynn. Leprévost gave a one parameter family of hyperelliptic curves with torsion order $2g^2+2g+1$ or $2g^2+3g+1$ in [Leprévost (1992)]. Then Flynn proved that fixing g, for any N in the interval $\left[g^2+2g+1, g^2+3g+1\right]$, there exists a hyperelliptic curve which contains a rational torsion divisor of order N in [Flynn (1991)]. There are similar results for order $2g^2+4g+1$ and $2g(2g+1)$. Moreover for $N=2g^2+5g+5$, Leprévost constructed a family of genus g hyperelliptic curves defined over $\mathbb{Q}$ such that their Jacobian have a rational torsion point of order N or $\frac{N}{2}$ or $\frac{N}{4}$, see [Leprévost (1997)].

In these articles the idea is similar to what we use in this work, we try to give two different descriptions of equations describing the same curve and use relations between divisors on hyperelliptic curves to obtain new torsion orders of rational points on the Jacobian of the curve.
By using this method, we can obtain small genus hyperelliptic curves such that their Jacobian has a torsion divisor of big order. Through this, we will obtain new torsion divisors that were not previously found in the literature.

Throughout this chapter, assume that K is a number field. Let $f(x) \in K[x]$ be a polynomial of odd degree $2g+1$ which has no repeated factors. We consider the hyperelliptic curve C described by the equation $y^2 = f(x)$. We let D be a divisor on C. We recall that the *Riemann-Roch* space of D is the K-vector space is given by

$$L(D) = \{\phi \in K(C) : \mathrm{div}(\phi) + D \geq 0\} \cup \{0\}$$

Assume that the set of the points of the curve over the number field K is denoted by $C(K)$. We notice that the curve C has one point at infinity, since the degree of $f(x)$ is odd, we eplained the details in the preliminary part. During this chapter we will denote the point at infiniy as P_∞. There exists a natural embedding of the curve C into its Jacobian J that maps a point P to the divisor class $[P-D]$,

where D is a fixed divisor of degree 1. As we explained in the background part, this map restricts to $C(k) \to J(k)$ if D is a k-rational divisor. In particular, one can choose D to be the rational divisor P_∞ if $f(x)$ is monic. The class of a divisor of the form $[P - P_\infty]$ defines an element in $J(K)$. We say that the divisor $[P - P_\infty]$ is a *torsion divisor* of order N if its class in the Jacobian J has order N. Notice that $K(C)$ is the function field, which consists of the functions on the curve C.

We remark that $\mathrm{ord}_{P_\infty}(x) = -2$ and $\mathrm{ord}_{P_\infty}(y) = -(2g+1)$. It follows that for any $m \geq 0$, if $D_m = 2(g+m+1)P_\infty$, then the genartors of Riemann-Roch space given by D_m is as follows:

$$L(D_m) = \langle 1, x, x^2, \cdots, x^{g+m+1}, y, xy, \cdots, x^m y \rangle$$

Moreover if $D'_m = (2(g+m)+1)P_\infty$, then the genartors of the Riemann-Roch space given by D'_m is as follows:

$$L(D'_m) = \langle 1, x, x^2, \cdots, x^{g+m}, y, xy, \cdots, x^m y \rangle$$

Let d, $0 \leq d \leq g-1$, be an integer. From now on, we work with the algebraic curves $C : y^2 = f(x)$ over the number field K where

$$f(x) = A(x)^2 - \lambda x^{g+1+d}(x-1)^{g-d}, \qquad A(x) \in K[x],\ \deg A(x) \leq g, \quad \lambda \in K \setminus \{0\}.$$

One sees that $P_0 = (0, A(0))$, $P_0{}' = (0, -A(0))$, $P_1 = (1, A(1))$, $P_1{}' = (1, -A(1))$ are in $C(K)$. In particular, the divisors $D_i = P_i - P_\infty$ and $D_i{}' = P_i{}' - P_\infty$, $i = 0, 1$, are K-rational divisors on C. We now consider $\phi_f \in K(C)$ such that

$$\mathrm{div}(\phi_f) = (g+m)P_0{}' + (g+m+2)P_1 - (2g+2m+2)P_\infty.$$

We notice that $\psi_f = \phi_f / x^{g+m} \in K(C)$ such that the divisor of ψ_f is given as follows:

$$\begin{aligned}
\mathrm{div}(\psi_f) &= \mathrm{div}(\phi_f / x^{g+m}) \\
&= \mathrm{div}(\phi_f) - \mathrm{div}(x^{g+m}) \\
&= (g+m)P_0{}' + (g+m+2)P_1 - (2g+2m+2)P_\infty \\
&- ((g+m)P_0{}' + (g+m)P_0 - (2g+2m)P_\infty) \\
&= -(g+m)P_0 + (g+m+2)P_1 - 2P_\infty
\end{aligned}$$

Moreover $y - A(x) \in K(C)$ and the divisor of this function can be obtained by

looking the equation of the curve as follows:

$$\operatorname{div}(y-A(x)) = (g+1+d)D_0 + (g-d)D_1$$

Therefore, one obtains the following system of equations

$$\begin{pmatrix} g+1+d & g-d \\ -(g+m) & (g+m+2) \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \end{pmatrix} = \begin{pmatrix} \operatorname{div}(y-A(x)) \\ \operatorname{div}(\psi_f) \end{pmatrix}. \tag{4.1}$$

Proposition 4.1 *Fix two integers $g \geq 1$ and d, $0 \leq d \leq g-1$. Let C be a hyperelliptic curve defined by the equation $y^2 = A(x)^2 - \lambda x^{g+1+d}(x-1)^{g-d}$, where $A(x) \in K[x]$, $\deg A(x) \leq g$, $\lambda \in K \setminus \{0\}$. Let m be an integer such that $1 \leq m < d+1$. Then there is a torsion divisor on C whose order divides $2g^2 + (2m+3)g + 2d + m + 2$.*

Proof. Assume that $M = \begin{pmatrix} g+1+d & g-d \\ -(g+m) & (g+m+2) \end{pmatrix}$. If we multiply both sides with $\det(M) \cdot M^{-1} \in \mathbb{Z}_{2\times 2}$, we obtain that $\det(M) \cdot D_0$ is a principal divisor, similar for D_1 also. This yields that $|D_0|$ and $|D_1|$ divide $\det(M) = 2g^2 + (2m+3)g + 2d + m + 2$. □

By investigating the divisor of ϕ_f, $\operatorname{div}(\phi_f) = (g+m){P_0}' + (g+m+2)P_1 - (2g+2m+2)P_\infty$, we can see that $\operatorname{div}(\phi_f) + (2g+2m+2)P_\infty \geq 0$. Then $\phi_f \in L((2g+2m+2)P_\infty)$. Thus, we deduce that $(\phi_f) = a(x) - b(x)y$ for some $a(x), b(x) \in K[x]$ such that $\deg a(x) \leq g+m+1$ and $\deg b(x) \leq m$.

In particular, one has that the norm of $\operatorname{div}(\phi_f)$ in $K(C)$ is given by

$$(a(x)-b(x)y)(a(x)+b(x)y) = h(x)x^{g+m}(x-1)^{g+m+2}, \quad h(x) \in K[x],\, u \in K \setminus \{0\}.$$

It follows that

$$\begin{aligned} a^2(x) - b^2(x)y^2 &= h(x)x^{g+m}(x-1)^{g+m+2} \\ a^2(x) - b^2(x)\left(A^2(x) - \lambda x^{g+1+d}(x-1)^{g-d}\right) &= h(x)x^{g+m}(x-1)^{g+m+2} \end{aligned}$$

$$\begin{aligned} a(x)^2 - b(x)^2A(x)^2 &= -\lambda b(x)^2 x^{g+1+d}(x-1)^{g-d} + h(x)x^{g+m}(x-1)^{g+m+2} \\ &= x^{g+m}(x-1)^{g-d}\left(h(x)(x-1)^{m+2+d} - \lambda b(x)^2 x^{d+1-m}\right) \end{aligned}$$

where $m < d+1$.

We know that $(\phi_f) = a(x) - b(x)y$ for some $a(x), b(x) \in K[x]$ such that $\deg a(x) \leq g+m+1$ and $\deg b(x) \leq m$ and $\operatorname{div}(\phi_f) = (g+m)P_0{}' + (g+m+2)P_1 - (2g+2m+2)P_\infty$. Since P_0 does not lie in the support of $\operatorname{div}(\phi_f)$ whereas $P_0{}'$ is in the support of $\operatorname{div}(\phi_f)$, it follows that $\phi_f(P_0) \neq 0$ and $\phi_f\left(P_0{}'\right) = 0$. Then $a(0) - b(0)A(0) \neq 0$ but $a(0) + b(0)A(0) = 0$. This yields that $x \nmid a(x) - b(x)A(x)$ whereas $x \mid a(x) + b(x)A(x)$. Similarly, the support of $\operatorname{div}(\psi_f)$ contains P_1 but it does not contain $P_1{}'$, therefore $(x-1) \mid a(x) - b(x)A(x)$ but $(x-1) \nmid a(x) + b(x)A(x)$. Thus, we may assume that

$$\begin{aligned} a(x) + b(x)A(x) &= p(x)x^{g+m}, \\ a(x) - b(x)A(x) &= q(x)(x-1)^{g-d}, \\ p(x)q(x) &= h(x)(x-1)^{m+2+d} - \lambda b(x)^2 x^{d+1-m}. \end{aligned}$$

It follows that

$$A(x) = \frac{p(x)^2 x^{g+m} - \left[h(x)(x-1)^{m+2+d} - \lambda b(x)^2 x^{d+1-m}\right](x-1)^{g-d}}{2p(x)b(x)} \tag{4.2}$$

where $A(x) \in K[x]$. We set $p(x) = x - \alpha$, $\alpha \neq 0, 1$, where α is to be chosen later such that $b(\alpha)$ and $h(\alpha)$ are non-zero, and $p(x) \mid \left(h(x)(x-1)^{m+2+d} - \lambda b(x)^2 x^{d+1-m}\right)$.

Now we will find conditions under which $b(x)$ divides the polynomial $p(x)^2 x^{g+m} - h(x)(x-1)^{g+m+2}$ of degree m. From now on, we assume that $g+m$ is even. We set $h(x) \equiv 1$. In the latter case, $p(x)^2 x^{g+m} - h(x)(x-1)^{g+m+2} = (p(x)x^{(g+m)/2} - (x-1)^{1+(g+m)/2})(p(x)x^{(g+m)/2} + (x-1)^{1+(g+m)/2})$. Now, we set $b(x) = p(x)x^{(g+m)/2} - (x-1)^{1+(g+m)/2}$.

Following the discussion above, we fix an integer m, $1 \leq m < d+1$, such that $g+m$ is even. We are interested in the following 1-parameter family of hyperelliptic curves

$$\begin{aligned} C_{\alpha,d} : y^2 &= \left(\frac{\lambda_{\alpha,d} b_\alpha(x) x^{d+1-m}(x-1)^{g-d} + (x-1)^{1+(g+m)/2} + (x-\alpha)x^{(g+m)/2}}{2(x-\alpha)}\right)^2 \\ &- \lambda_{\alpha,d} x^{g+1+d}(x-1)^{g-d}, \\ b_\alpha(x) &= (x-\alpha)x^{(g+m)/2} - (x-1)^{1+(g+m)/2}, \quad \alpha \neq 0, 1, \\ \lambda_{\alpha,d} &= \frac{1}{\alpha^{d+1-m}(\alpha-1)^{g-d}}. \end{aligned}$$

One sees that $\deg(b_\alpha(x)) = (g+m)/2$ if $\alpha \neq (g+m)/2+1$, whereas $\deg(b_\alpha(x)) = (g+m)/2-1$ otherwise. Since $\deg(b_\alpha(x))$ is at most m and $\deg A(x) = g$, the possible values for m are either g and then $\alpha \neq g+1$; or $g-2$ where in this case $\alpha = g$. The fact that $m < d+1 \leq g$ implies that $m = g-2$, hence $\alpha = g$ and $b_\alpha(x) = b_g(x) =$

$(x-g)x^{g-1}-(x-1)^g$.

4.1 The order of the torsion divisor

In this section, we discuss the order of the torsion subgroup of the Jacobian of the curve $C_{\alpha,d}$ defined above when $\alpha = g$. We notice that in this case, d is either $g-2$ or $g-1$. We will show that the curve $C_{g,d}$ is indeed hyperelliptic of genus g.

Proposition 4.2 *Fix an integer $g \geq 2$. The curves $C^t_{g,g-2}$ and $C^t_{g,g-1}$ defined over $\mathbb{Q}(t)$ by*

$$\begin{aligned} C^t_{g,g-1} &: y^2 = A^t_{g-1}(x)^2 - 4tx^{2g}(x-1), \\ C^t_{g,g-2} &: y^2 = A^t_{g-2}(x)^2 - 4tx^{2g-1}(x-1)^2, \end{aligned}$$

where

$$\begin{aligned} A^t_{g-1}(x) &= \frac{(x-g)x^{g-1}+(x-1)^g+tx^2(x-1)\left((x-g)x^{g-1}-(x-1)^g\right)}{(x-g)}, \\ A^t_{g-2}(x) &= \frac{(x-g)x^{g-1}+(x-1)^g+tx(x-1)^2\left((x-g)x^{g-1}-(x-1)^g\right)}{(x-g)} \end{aligned}$$

are hyperelliptic curves of genus g.

Proof. We set

$$f^t_{g-1}(x) = ((x-g)A^t_{g-1}(x))^2 - 4tx^{2g}(x-1)(x-g)^2 \in \mathbb{Q}(t)[x].$$

We need to prove that the discriminant of $f^t_{g-1}(x)$, $\Delta\left(f^t_{g-1}(x)\right)$, is nonzero. We assume on the contrary that $f^t_{g-1}(x) = P^t_1(x)\cdot P^t_2(x)^2$ for some $P^t_1(x)$ and $P^t_2(x)$ in $\mathbb{Q}[t,x]$ where $P^t_1(x)$ is square-free as a polynomial in x. Since $\deg_t\left(f^t_{g-1}\right)=2$, one sees that the ordered pair $\left(\deg_t\left(P^t_1(x)\right),\deg_t\left(P^t_2(x)\right)\right)$ is either $(0,1)$ or $(2,0)$. Assuming that $\left(\deg_t\left(P^t_1(x)\right),\deg_t\left(P^t_2(x)\right)\right)=(0,1)$, it follows that each t^i-coefficient of $f^t_{g-1}(x)$, as a polynomial in t, is divisible by $P_1(x) := P^t_1(x)$, $i=0,1,2$.

In particular, one obtains that

$$\begin{aligned} P_1(x) &\mid 2\Big((x-g)x^{(g-1)}+(x-1)^g\Big)\Big(x^2\cdot(x-1)\cdot\Big((x-g)x^{g-1}-(x-1)^g\Big)\Big) \\ &+ 4x^{2g}(x-1)(x-g)^2, \\ P_1(x) &\mid \Big((x-g)x^{(g-1)}+(x-1)^g\Big)^2. \end{aligned}$$

The divisibility conditions above imply that $P_1(x) \mid 4x^{2g}(x-1)(x-g)^2$, in particular, $P_1(x) \mid 2x(x-1)(x-g)$. Yet, the last divisibility condition implies that $x, x-1, x-g$ cannot be factors of $P_1(x)$ if $g \geq 2$. Therefore, $f^t_{g-1}(x)$ is either $P^t_2(x)^2$ or $2P^t_2(x)^2$. This is a contradiction as $f^t_{g-1}(x)$ is of odd degree as a polynomial in x.

We now assume that $\Big(\deg_t\Big(P^t_1(x)\Big), \deg_t\Big(P^t_2(x)\Big)\Big) = (2,0)$. It follows that $P^t_2(x)$ divides each t^i-coefficient of $f^t_{g-1}(x)$, as a polynomial in t, $i = 0,1,2$. A contradiction is obtained by following the same argument as in the previous case.

The proof that the curve $C^t_{g,g-2}$ is of genus g over $\mathbb{Q}(t)$ is similar. □

Theorem 4.1 *Fix an integer $g \geq 2$. We set $t_g = 1/(g^2(g-1))$ and $s_g = 1/(g(g-1)^2)$. We consider the following curves of genus g defined over $\mathbb{Q}$ by the equations*

$$\begin{aligned} C_{g,g-1} &: y^2 = f_{t_g}(x) := A_{g-1}(x)^2 - 4t_g x^{2g}(x-1), \\ C_{g,g-2} &: y^2 = f_{s_g}(x) = A_{g-2}(x)^2 - 4s_g x^{2g-1}(x-1)^2, \end{aligned}$$

where

$$\begin{aligned} A_{g-1}(x) &= \frac{(x-g)x^{g-1}+(x-1)^g+t_g x^2(x-1)\Big((x-g)x^{g-1}-(x-1)^g\Big)}{(x-g)}, \\ A_{g-2}(x) &= \frac{(x-g)x^{g-1}+(x-1)^g+s_g x(x-1)^2\Big((x-g)x^{g-1}-(x-1)^g\Big)}{(x-g)}. \end{aligned}$$

There is a torsion divisor on the curve $C_{g,g-1}$, respectively $C_{g,g-2}$, whose order is $4g^2+2g-2$, respectively $4g^2+2g-4$.

Proof. That the curves $C_{g,g-1}$ and $C_{g,g-2}$ are of genus g over $\mathbb{Q}$ follows from Proposition 4.2. We recall the existence of the following rational functions on the curve

$C_{g,g-1}$

$$\begin{aligned}
\phi_{f_{t_g}} &= a_{g-1}(x) - b_{g-1}(x)y,\\
\psi_{f_{t_g}} &= \frac{\phi_{f_{t_g}}}{x^{g+m}} = \frac{a_{g-1}(x) - b_{g-1}(x)y}{x^{g+m}},\\
\theta_{f_{t_g}} &= y - A_{g-1}(x),
\end{aligned}$$

where the norm of $\phi_{f_{t_g}}$ is given by $a_{g-1}^2(x) - b_{g-1}^2(x)y^2 = x^{g+m}(x-1)^{g+m+2} = x^{2g-2}(x-1)^{2g}$. According to Proposition 4.1, the order of the class of the divisor $D_0 = (0, A_{g-1}(0)) - P_\infty$ divides $l = 4g^2 + 2g - 2$. It follows that the principal divisor lD_0 is the divisor of the rational function $L_{g-1}(x,y)$ where

$$L_{g-1}(x,y) = \frac{{\theta_{f_{t_g}}}^{g+m+2}}{{\psi_{f_{t_g}}}^{g-d}} = \frac{{\theta_{f_{t_g}}}^{2g} \cdot x^{2g-2}}{\phi_{f_{t_g}}} = \frac{(y - A_{g-1}(x))^{2g} x^{2g-2}}{a_{g-1}(x) - b_{g-1}(x)y}. \tag{4.3}$$

This implies that

$$\begin{aligned}
L_{g-1}(x,y) =& \frac{(y - A_{g-1}(x))^{2g} \cdot (a_{g-1}(x) + b_{g-1}(x)y) \cdot x^{2g-2}}{a_{g-1}(x)^2 - b_{g-1}(x)^2 y^2}\\
=& \frac{(y - A_{g-1}(x))^{2g} \cdot (a_{g-1}(x) + b_{g-1}(x)y) \cdot x^{2g-2}}{(x-1)^{2g} \cdot x^{2g-2}}\\
=& \frac{(y - A_{g-1}(x))^{2g} \cdot (a_{g-1}(x) + b_{g-1}(x)y)}{(x-1)^{2g}} \qquad (4.4)
\end{aligned}$$

We recall that ${P_1}' = (1, -A_{g-1}(1)), {P_0}' = (0, -A_{g-1}(0)) \in C_{g,g-1}(\mathbb{Q})$ do not appear in the support of the divisor D_0. From equations (4.3) and (4.4) describing $L_{g-1}(x,y)$, we can compute $L_{g-1}\left({P_1}'\right)$ and $L_{g-1}\left({P_0}'\right)$ as follows

$$\begin{aligned}
L_{g-1}\left({P_1}'\right) &= \frac{(-2A_{g-1}(1))^{2g} \cdot 1^{2g-1}}{a_{g-1}(1) + b_{g-1}(1)A_{g-1}(1)} = \frac{2^{2g}}{(1-g)},\\
L_{g-1}\left({P_0}'\right) &= \frac{(-2A_{g-1}(0))^{2g} \cdot (a_{g-1}(0) - b_{g-1}(0)A_{g-1}(0))}{(-1)^{2g}}\\
&= \frac{2^{2g}.}{(-g)^{2g} \cdot g \cdot (-1)^{2g}} = \frac{2^{2g}}{g^{2g+1}}.
\end{aligned}$$

We therefore obtain the following identity

$$L_{g-1}\left({P_1}'\right)(1-g) = L_{g-1}\left({P_0}'\right) g^{2g+1}.$$

Assume that the order of the D_0 is f then $l = j \cdot f$ for some $j \in \mathbb{N}$. So we can say that there exists a rational function N_{g-1} on the curve $C_{g,g-1}$ such that $fD_0 = (N_{g-1})$. Moreover, we know that $j \cdot fD_0 = lD_0 = (L_{g-1})$. Hence we obtain that $L_{g-1} = aN_{g-1}^j$,

for some $a \in \mathbb{Q}$. Therefore we manage to find the following equality:

$$N_{g-1}^{j}\left(P_1{}'\right)(1-g) = N_{g-1}^{j}\left(P_0{}'\right) g^{2g+1}.$$

If we look at right hand side of the equation we have g as a factor and left hand side we have $1-g$, which are relatively prime. The valuation of g is $2g+1+j\cdot c$ for some $c \in \mathbb{Z}$, on the right-hand side of the equation. But on the left-hand side it can be $j \cdot c'$, for some $c' \in \mathbb{Z}$. Then $2g+1 = j(c'-c)$. Then j must divide $2g+1$. We also know that $j \cdot f = l = 4g^2+2g-2 = 2(2g-1)(g+1)$. Given that $2g+1$ is relatively prime to $l = 4g^2+2g-2 = 2(2g-1)(g+1)$, this implies that the order of the class of D_0 cannot be a proper divisor of l, and hence must be l itself.

For the curve $C_{g,g-2}$, we set $\phi_{f_{sg}} = a_{g-2}(x) - b_{g-2}(x)y$, $\psi_{f_{sg}} = \phi_{f_{sg}}/x^{g+m}$, and $\theta_{f_{sg}} = y - A_{g-2}(x)$. We consider the class of divisor $D_1 := P_1 - P_\infty$, where $P_1 = (1, A_{g-2}(1))$. According to Proposition 4.1, there is a rational function $L_{g-2}(x,y)$ defined in $C_{g,g-2}$ such that the principal divisor $l'D_1$ is the divisor of L_{g-2}, where $l' = 4g^2+2g-4$. In fact, the function L_{g-2} is defined as follows.

$$\begin{aligned}
L_{g-2}(x,y) &= \theta_{f_{sg}}^{2g-2} \cdot \psi_{f_{sg}}^{2g-1} \\
&= \frac{\theta_{f_{sg}}^{2g-2} \cdot \phi_{f_{sg}}^{2g-1}}{x^{(2g-1)\cdot(2g-2)}} \\
&= \frac{(y - A_{g-2}(x))^{2g-2} \cdot (a_{g-2}(x) - b_{g-2}(x)y)^{2g-1}}{x^{(2g-1)\cdot(2g-2)}} \qquad (4.5) \\
&= \frac{(y - A_{g-2}(x))^{2g-2} \cdot (a_{g-2}(x) - b_{g-2}(x)y)^{2g-1} \cdot (a_{g-2}(x) + b_{g-2}(x)y)^{2g-1}}{x^{(2g-1)(2g-2)} \cdot (a_{g-2}(x) + b_{g-2}(x)y)^{2g-1}} \\
&= \frac{(y - A_{g-2}(x))^{2g-2} \cdot \left(a_{g-2}^2(x) - b_{g-2}^2(x)y^2\right)^{2g-1}}{x^{(2g-1)(2g-2)} \cdot (a_{g-2}(x) + b_{g-2}(x)y)^{2g-1}} \\
&= \frac{(y - A_{g-2}(x))^{2g-2} \cdot x^{(2g-2)\cdot(2g-1)} \cdot (x-1)^{(2g-4)(2g-1)}}{x^{(2g-2)(2g-1)} \cdot (a_{g-2}(x) + b_{g-2}(x)y)^{2g-1}} \\
&= \frac{(y - A_{g-2}(x))^{2g-2} \cdot (x-1)^{(2g-4)\cdot(2g-1)}}{(a_{g-2}(x) + b_{g-2}(x)y)^{2g-1}} \qquad (4.6)
\end{aligned}$$

For the points $P_1{}' = (1, -A_{g-2}(1)), P_0{}' = (0, -A_{g-2}(0)) \in C_{g,g-2}(\mathbb{Q})$, we use equa-

tions (4.5) and (4.6) to compute $L_{g-2}\left(P_1{}'\right)$ and $L_{g-2}\left(P_0'\right)$ respectively as follows

$$L_{g-2}\left(P_1{}'\right) = \frac{(-2A_{g-2}(1))^{2g-2}\cdot(1-g)^{2g-1}}{1^{(2g-1)\cdot(2g-2)}} = 2^{2g-2}(1-g)^{2g-1},$$
$$L_{g-2}\left(P_0{}'\right) = \frac{(-2A_{g-2}(0))^{2g-2}\cdot(-1)^{(2g-4)\cdot(2g-1)}}{(a(0)-b(0)A_{g-2}(0))^{2g-1}} = \frac{2^{2g-2}\cdot\left(\frac{1}{g}\right)^{2g-2}}{\left(\frac{-1}{g}\right)^{2g-1}} = -2^{2g-2}\cdot g.$$

We obtain the following equality:

$$-gL_{g-2}\left(P_1{}'\right) = (1-g)^{2g-1}L_{g-2}\left(P_0{}'\right)$$

Analogous to the previous argument, we may assume that the order of D_1 is f with $j\cdot f = l$ for some $j\in\mathbb{Q}$. Then there exists a rational function N_{g-2} on the curve $C_{g,g-2}$ such that $fD_1 = (N_{g-2})$. Moreover, we know that $j\cdot fD_1 = lD_1 = (L_{g-2})$. Hence we obtain that $L_{g-2} = aN_{g-2}^j$, for some $a\in\mathbb{Q}$. Therefore we have the following equality:

$$-gN_{g-2}^j\left(P_1{}'\right) = (1-g)^{2g-1}N_{g-2}^j\left(P_0{}'\right)$$

The valuation of $1-g$ is $2g-1+j\cdot c$ for some $c\in\mathbb{Z}$, on the right-hand side of the equation. But on the left-hand side it can be $j\cdot c'$, for some $c'\in\mathbb{Z}$. Then we obtain $2g-1 = j(c'-c)$. Then j must divide $2g-1$. We also know that $j\cdot f = l = 4g^2+2g-4 = 2(2g-1)(g+1)-2$. We observe that $2g-1$ is relatively prime to $4g^2+2g-4 = 2(2g-1)(g+1)-2$ implies that the order of class of the divisor of D_1 is exactly $4g^2+2g-4$. □

In the following example, we produce hyperelliptic curves of genus g, $2\le g\le 5$, whose Jacobians possess rational torsion points with order determined by Theorem 4.1.

Example 4.1 *Consider the genus-2 hyperelliptic curve C_2 described by $y^2 = -16x^5+17x^4-14x^3+53x^2-28x+4$, the order of the class of the divisor $D_0 = (0:2:1)-(1:0:0)$ is 18 and the class of the divisor $D_1 = (1:4:1)-(1:0:0)$ is of order 9.*

For the genus-2 hyperelliptic curve $C_2{}'$ described by $y^2 = -8x^5+17x^4-16x^3+18x^2-8x+1$, the order of $D_1 = (1:2:1)-(1:0:0)$ is 16 and the order of $D_0 = (0:1:1)-(1:0:0)$ is 8.

Consider the genus-3 hyperelliptic curve C_3 described by $y^2 = -72x^7+81x^6-186x^5+1057x^4-1028x^3+628x^2-192x+36$. The class of the divisor $D_0 = (0:6:1)-(1:0:0)$ is of order 40 in the Jacobian of the curve C_3. One also notices that the class of

the divisor $D_1 = (1:18:1) - (1:0:0)$ *is of order* 20. *According to [Nicholls (2018)], this is the first example of a genus-*3 *hyperelliptic curve with a rational torsion point of order* 20 *on its Jacobian.*

The class of the divisor $D_0 = (0:12:1) - (1:0:0)$ *has order* 70 *in the Jacobian of the genus-*4 *curve* $C_4 : y^2 = -192x^9 + 228x^8 - 984x^7 + 7456x^6 - 10544x^5 + 11245x^4 - 7458x^3 + 3489x^2 - 1080x + 144$. *This is the first example of a genus-*4 *curve with a rational divisor of order* 70 *on its Jacobian.*

The class of the divisor $D_0 = (0:20:1) - (1:0:0)$ *has order* 108 *in the Jacobian of the genus-*5 *curve* $C_5 : y^2 = -400x^{11} + 500x^{10} - 3400x^9 + 32200x^8 - 59720x^7 + 90685x^6 - 92770x^5 + 71241x^4 - 41352x^3 + 16456x^2 - 3840x + 400$.

The class of the divisor $D_1 = (2:1280:1) - (1:0:0)$ *has order* 106 *in the Jacobian of the genus-*5 *curve* ${C_5}' : y^2 = -40x^{11} + 185x^{10} - 1560x^9 + 22300x^8 - 81440x^7 + 242580x^6 - 490400x^5 + 745376x^4 - 857728x^3 + 678464x^2 - 315392x + 65536$.

4.2 An infinite family of hyperelliptic curves

Lemma 4.1 *Let* $g \geq 2$ *be an integer. There exists a family of hyperelliptic curves such that the Jacobian has a rational torsion divisor of order divides* $2g^2+5g+2d+3$, *for some integer* d *between* $-g-1 < d < g$, *on its Jacobian.*

Proof. Consider $C := y^2 = A^2(x) - \lambda x^{g+1+d}(x-1)^{g-d}$, whic is a hyeprelliptic curve. Then one sees that $P_0 = (0, A(0))$, ${P_0}' = (0, -A(0))$, $P_1 = (1, A(1))$, ${P_1}' = (1, -A(1))$ are in $C(K)$, as previous case. We will prove that there exists ψ on C such that $\mathrm{div}(\psi) = -(g+1)D_0 + (g+3)D_1$. It follows that

$$\det(M) = \begin{vmatrix} (g+1+d) & (g-d) \\ -(g+1) & (g+3) \end{vmatrix} = 2g^2+5g+2d+3$$

Here, instead of existing of ψ, it will be enough to have φ on C such that

$$\mathrm{div}(\varphi) = (g+1){P_0}' + (g+3)P_1 - (2g+4)P_\infty$$

Since $\mathrm{div}\left(\varphi/x^{g+1}\right) = \mathrm{div}(\psi)$. We know that $\varphi \in L((2g+4)P_\infty) = \left\langle 1, x, x^2, \ldots, x^{g+2}, y, xy \right\rangle$. Then $\varphi = a(x) - b(x)y$ where $a(x)$ and $b(x)$ are some

rational polynomials with $\deg(a(x)) \leq g+2$ and $\deg(b(x)) \leq 1$. Moreover, we have that $(a(x)-b(x)y)((a(x)+b(x)y) = k \cdot x^{g+1}(x-1)^{g+3}$, by looking at the divisor of φ. Then we have the following equalities:

$$\begin{aligned} a^2(x) - b^2(x)y^2 &= kx^{g+1}(x-1)^{g+3} \\ a^2(x) - b^2(x)A^2(x) &= x^{g+1}(x-1)^{g-d}\left[k(x-1)^{d+3} - \lambda b^2(x)x^d\right] \end{aligned}$$

One assumes that both sides of the polynomials are monic, so say that $k=1$. Since $\mathrm{div}(\varphi)$ does not contain P_0, but contains $P_0{}'$ then $\varphi(P_0) \neq 0$ but $\varphi(P_0{}') = 0$. This implies that $x \nmid a(x)-b(x)A$ but $x \mid a(x)+b(x)A$. Similarly, $\varphi(P_1) = 0$ but $\varphi(P_1') \neq 0$. Then $(x-1) \mid a(x)-b(x)A$ but $(x-1) \nmid a(x)+b(x)A$. It follows that

$$\begin{aligned} a(x) - b(x)A &= (x-1)^{g-d} \cdot q \\ a(x) + b(x)A &= x^{g+1} \cdot p \end{aligned}$$

where $p \cdot q = (x-1)^{d+3} - \lambda b^2(x)x^d$. We need to have that $\deg(p) = 1$, and $\deg(q) = d+2$. Since $\deg((a(x)-b(x)A) \leq g+2$ and $\deg(a(x)+b(x)A) \leq g+2$.

Since p and $b(x)$ are degree one monic polynomials, $p = x-\alpha$ and $b(x) = x-\beta$, for some $\beta, \alpha \in \mathbb{Q}$. Then

$$A = \frac{x^{g+1}(x-\alpha)^2 - \left[(x-1)^{g-d}\left((x-1)^{d+3} - \lambda(x-\beta)^2x^d\right)\right]}{2 \cdot (x-\alpha)(x-\beta)}.$$

As A is a polynomial in $\mathbb{Q}[x]$, we obtain two following equations:

i) $(\alpha-1)^{g-d}\left((\alpha-1)^{d+3} - \lambda(\alpha-\beta)^2\alpha^d\right) = 0$

ii) $\beta^{g+1}(\beta-\alpha)^2 - (\beta-1)^{g+3} = 0.$

To satisfy the first equation we can choose $\lambda = \frac{(\alpha-1)^{d+3}}{(\alpha-\beta)^2\alpha^d}$ where $\alpha \neq \beta$ and $\alpha \neq 0$ and $(\beta-\alpha)^2 = \frac{(\beta-1)^{g+3}}{\beta^{g+1}}$. If g is odd then we can choose α as follows.

$$(\beta-\alpha) = \pm\frac{(\beta-1)^{\frac{g+3}{2}}}{\beta^{\frac{g+1}{2}}} \Rightarrow \alpha \quad = \beta \pm \frac{(\beta-1)^{\frac{g+3}{2}}}{\beta^{\frac{g+1}{2}}}.$$

By looking at the degree of the monomials of the equation $y^2 = A^2(x) - \lambda x^{g+1+d}(x-1)^{g-d}$ describing the curve, we need to have $-g-1 < d < g$. □

Theorem 4.2 *Fix an odd integer $g \geq 2$. We set*

$$\alpha = \beta - \frac{(\beta-1)^{\frac{g+3}{2}}}{\beta^{\frac{g+1}{2}}}, \beta \neq 0, 1, \quad \lambda = \frac{(\alpha-1)^{g+2}}{(\alpha-\beta)^2\alpha^{g-1}} \in \mathbb{Q}(\beta).$$

The family of hyperelliptic curves C_β of genus g defined over $\mathbb{Q}(\beta)$ by the equation

$$y^2 = A^2(x) - \lambda x^{2g}(x-1)$$

where

$$A(x) = \frac{x^{g+1}(x-\alpha)^2 - \left[(x-1)\left((x-1)^{g+2} - \lambda(x-\beta)^2 x^{g-1}\right)\right]}{2(x-\alpha)(x-\beta)} \in \mathbb{Q}(\beta)[x],$$

possesses a torsion divisor whose order is $2g^2+7g+1$.

Proof. The proof follows the same ideas in the proof of Theorem 4.1. Assume that $y^2 = A^2(x) - \lambda x^{2g}(x-1)$ where

$$A(x) = \frac{x^{g+1}(x-\alpha)^2 - \left[(x-1)\left((x-1)^{g+2} - \lambda(x-\beta)^2 x^{g-1}\right)\right]}{2(x-\alpha)(x-\beta)},$$
$$\lambda = \frac{(\alpha-1)^{g+2}}{(\alpha-\beta)^2\alpha^{g-1}} \text{ and } \alpha = \beta - \frac{(\beta-1)^{\frac{g+3}{2}}}{\beta^{\frac{g+1}{2}}}.$$

By Lemma 4.1 the order of D_0 divides $l = 2g^2+7g+1$. Assume that $\theta(x) = y - A(x)$ and $\varphi(x) = a(x) - b(x)y, \psi(x) = \dfrac{\varphi(x)}{x^{g+1}}$.

Let $L(x,y)$ be a function of the divisor of $lD0$ where $l = 2g^2+7g+1$. This function is defined by

$$L(x,y) = \frac{\theta(x)^{g+3}}{\Psi} = \frac{\theta(x)^{g+3}}{\varphi}x^{g+1} = \frac{x^{g+1}\cdot\theta(x)^{g+2}(\theta(x)\tilde{\varphi})}{\varphi\cdot\tilde{\varphi}}$$

where $\tilde{\varphi} = a(x) + b(x)y$, then $\varphi\cdot\tilde{\varphi} = a^2(x) - b^2(x)y^2 = x^{g+1}(x-1)^{g+3}$

$$\begin{aligned}
\text{Moreover } \tilde{\varphi}\cdot\theta(x) &= (y - A(x))(a(x) + b(x)y) \\
&= b(x)y^2 + a(x)y - a(x)A(x) - b(x)A(x)y \\
&= (x-\beta)y^2 - A(x)a(x) + y(a(x) - b(x)A(x)) \\
&= (x-\beta)y^2 - A(x)a(x) + (x-1)\cdot q\cdot y4.2 \\
\text{Since } (x-\beta)y^2 - A(x)a(x) &= (x-\beta)\left[A^2(x) - \lambda x^{2g}(x-1)\right] - A(x)a(x) \\
&= (x-\beta)A^2(x) - \lambda x^{2g}(x-1)(x-\beta) - A(x)(x-1)q - (x-\beta)A^2(x) \\
&= -\lambda x^{2g}(x-1)(x-\beta) - (x-1)A(x)\cdot q
\end{aligned}$$

Then $\tilde{\varphi}\cdot\theta(x) = (x-1)\left[q\cdot(y - A(x)) - \lambda x^{2g}(x-\beta)\right]$

As a result

$$L(x,y) = \frac{(y-A(x))^{g+2}\left[q(y-A(x)) - \lambda x^{2g}(x-\beta)\right]}{(x-1)^{g+2}}. \tag{4.7}$$

Assume that the class of D_0 is not the order l. Then $l = mn$ where m and n are integer divisors of l and D_0 is of order n, i.e. there exists a rational function $N(x,y)$ on $\mathbb{Q}(\beta)$ such that

$$nD_0 = (N).$$

Then there exists a constant s, such that $sN^m(x,y) = L(x,y)$. Since $P_0' = (0, -A(0))$ and $P_1 = (1, A(1))$ are not in the support of the divisor D_0, then

$$\frac{L(P_0')}{L(P_1)} = \frac{N^m(P_0')}{N^m(P_1)}$$

$$L\left(P_0'\right) = \frac{q(0)(-2A(0))^{g+3}}{(-1)^{9+2}} \text{ , where } q = \frac{(x-1)^{g+2} - \lambda(x-\beta)^2 x^{9-1}}{(x-\alpha)}$$

Then $L(P_0') = \dfrac{(-2A(0))^{g+3}}{-\alpha} = \dfrac{1}{\alpha^{g+4}\beta^{g+3}}$.
Moreover,

$$\begin{aligned}
L(x,y) &= \frac{L(x,y)\cdot\bar{\theta}(x,y)^{g+2}}{\bar{\theta}(x,y)^{g+2}}, \text{ where } L(x,y) \text{ can be given by equation (4.7)} \\
&= \frac{\left[y^2 - A^2(x)\right]^{g+2} \cdot \left[q(y-A(x)) - \lambda x^{2g}(x-\beta)\right]}{(x-1)^{g+2}(y+A(x))^{g+2}} \\
&= \frac{\left[-\lambda x^{2g}(x-1)\right]^{g+2}\left[q(y-A(x)) - \lambda x^{2g}(x-\beta)\right]}{(x-1)^{g+2}(y+A(x))^{g+2}} \\
&= \frac{\left(-\lambda x^{2g}\right)^{g+2}\left[q(y-A) - \lambda x^{2g}(x-\beta)\right]}{(y+A(x))^{g+2}}
\end{aligned}$$

Evaluate $P_1 = (1, A(1))$ at $L(x,y)$ we obtain:

$$
\begin{aligned}
L(P_1) &= \frac{(-\lambda)^{g+3}(1-\beta)}{(2A(1))^{g+2}} \quad \text{since g is odd} \\
&= \frac{\lambda^{g+3}(1-\beta)^{g+3}}{(1-\alpha)^{g+2}} \\
&= \frac{\lambda^{g+3}(1-\beta)^{g+3}}{-\lambda\cdot\alpha^{g-1}(\alpha-\beta)^2}, (\text{ since } \alpha-\beta = \frac{(\beta-1)^{\frac{g+3}{2}}}{\beta^{\frac{g+1}{2}}}) \\
&= \frac{-\lambda^{g+1}\cdot\beta^{g+1}}{\alpha^{g-1}}.
\end{aligned}
$$

Consequently, we obtain

$$\frac{L(P_0')}{L(P_1)} = -\beta^{2g+4}\alpha^5\lambda^{g+1}$$

which is the polynomial of β with degree $3g+10$. Since $3g+10$ is coprime with $2g^2+7g+1$, by following the same argument with the previous proofs we conclude that the order of D_0 is exactly equals to $l = 2g^2+7g+1$.

□

Example 4.2 *Consider the genus-3 hyperelliptic curve described by* $y^2 = -190512x^7 + 727801x^6 - 1181596x^5 + 1054252x^4 - 527008x^3 + 166448x^2 - 30912x + 3136$. *The class of the divisor* $D_0 = (0:56:1) - (1:0:0)$ *is of order* 40 *in the Jacobian of the hyperelliptic curve. We remark that this curve is not isomorphic to the genus-3 curve* C_3 *given in Example 4.1.*

Consider the genus-5 hyperelliptic curve defined by $y^2 = -1334139660000x^{11} + 7810111072849x^{10} - 21237895715004x^9 + 35509499052172x^8 - 40961959673568x^7 + 34980786907216x^6 - 22600090770240x^5 + 11170251259200x^4 - 4105259712000x^3 + 1045133280000x^2 - 162518400000x + 11664000000$. *The class of the divisor* $D_0 = (0:108000:1) - (1:0:0)$ *gives rise to a rational point of order* 86 *in the Jacobian of the curve. This curve corresponds to* $\beta = 2$ *and* $g = 5$ *in Theorem 4.2.*

Corollary 4.1 *In Theorem 4.2, we set* $\beta = u(t) := (t^2+1)^2/4t^2$, $t \neq 0, 1$. *For any integer* $g \geq 2$, *the curve* $C_{u(t)}$ *is a hyperelliptic curve of genus* g *defined over* $\mathbb{Q}(t)$ *that possesses a torsion divisor whose order is* $2g^2+7g+1$.

Consider the genus-2 hyperelliptic curve described by $y^2 = -299054816676000x^5 + 937313042871529x^4 - 1165161421194050x^3 + 677279473485625x^2 - 132825168000000x + 8294400000000$. The class of $D_0 = (0:2880000:1) - (1:0:0)$ is of order 23. This curve corresponds to $t = 2$ and $\beta = 25/16$ in Corollary 4.1.

Consider the genus-4 hyperelliptic curve described by

$$
\begin{aligned}
y^2 &= -4410764513139682083438616677713721000000x^9 \\
&+ 22310095034036707025629820436058652226 49x^8 \\
&- 4959972109544667027708192318400142478050x^7 \\
&+ 6329054704630532302814017899191191335625x^6 \\
&- 5260199601304122072610634289700416000000x^5 \\
&+ 3123070596609213073858989244272000000000x^4 \\
&- 1315926242281486797139217238210000000000x^3 \\
&+ 396345305950692328102018752000000000000x^2 \\
&- 767866922909156143166688000000000000000x \\
&+ 673382222718848052804000000000000000000
\end{aligned}
$$

The class of $D_0 = (0 : 2594960929800000000 : 1) - (1 : 0 : 0)$ is of order 61. This curve corresponds to $t = 2$ and $\beta = 25/16$.

4.3 Cubic Order

In this part, we will discuss the question of whether it's possible to construct hyperelliptic curves with a rational torsion point whose order is cubic, in relation to the genus.

To obtain this torsion order, intuitively we need to obtain 3×3 matrices. So, in this case we are taking $y^2 = f(x)$, with $\deg(f(x)) = 2g + 2$. Then we have two points at infinity, by this way we have D_∞ as a divisor, unlike rational divisors in the 2×2 case. Actually the idea in the previous part is finding two different ways to write the equation describing the curve. Now our aim is to find 3 different ways to represent the curve. Leprévost is constructing genus 2 curves with torsion $N = 21, 22, 23, 25, 26, 27, 29$ by using this method [Leprévost (1995)]. We are giving an example of a family of genus 3 hyperelliptic curves with torsion order 25.

Assume that $y^2 = f(x) = A^2(x) - \lambda x^i(x-1)^j$ where $i + \dot{j} \leqslant 2g + 1$, $i, j \in \mathbb{Z}$ and $A(x) \in \mathbb{R}[x]$ with degree is $g + 1$. So here we have an even degree curve, that is there exits two points of infinity denoted by ${P_\infty}^-$ and ${P_\infty}^+$. We have the rational points on the curve as $P_0 = (0, A(0)), P_1 = (1, A(1)), {P_0}' = (0, -A(0))$,

$P_1' = (1, -A_1)), P_\infty{}^+$ and $P_\infty{}^-$, which give us the following rational divisors:

$$\begin{aligned} D_0 &= P_0 - P_\infty{}^+ \\ D_1 &= P_1 - P_\infty{}^+ \\ D_\infty &= P_\infty{}^- - P_\infty{}^+. \end{aligned}$$

Assume that there exists another way to write the curve equation as follows:

$$y^2 = f(x) = B^2(x) - \mu x^k (x-1)^l \text{ with}$$

$k+l \leq 2g+1$ and $B(x) \in \mathbb{R}[x]$ with degree is $g+1$. Then $A(0) = \pm B(0)$ and $A(1) = \pm B(1)$.

Our aim is to find another equation of the curve as $y^2 = C^2(x) - \lambda x^m (k-1)^n$, by this way we will obtain the functions which are obtained by $y - A(x), y - B(x)$ and $y - C(x)$, let's call them ϕ_1, ϕ_2, ϕ_3 respectively. Then this will gives us the following equation:

$$\begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{pmatrix} \begin{pmatrix} D_0 \\ D_1 \\ D_\infty \end{pmatrix} = \begin{pmatrix} \operatorname{div}(\phi_1) \\ \operatorname{div}(\phi_2) \\ \operatorname{div}(\phi_3) \end{pmatrix}$$

So by the same argument with the previous section the order of D_0, D_1 and D_∞ divide $\det(M)$.

Example 4.3 *Assume that*

$$\begin{aligned} y^2 &= A^2(x) + mx^4(x-1) \\ &= B^2(x) + nx^3(x-1) \\ &= C^2(x) + rx. \end{aligned}$$

Then $(B-A)(B+A) = x^3(x-1)(mx-n)$. *Assume that* $B(1) = A(1)$ *and* $B(0) = -A(0)$. *Then*

$$\begin{aligned} A(x) &= \frac{ux^2(mx-n)}{2} - \frac{x-1}{2v} \\ B(x) &= \frac{ux^3(mx-n)}{2} + \frac{x-1}{2v} \text{ for some } u \in \mathbb{Q} \end{aligned}$$

Moreover $(C-A)(C+A) = x(x-1)(mx^3(x-1)-r)$, *assume that* $A(0) = -C(0)$.

Then

$$A(x) = \frac{v\left(mx^3(x-1)-r\right)}{2} - \frac{x}{2v}$$
$$C(x) = \frac{v\left(mx^3(x-1)-r\right)}{2} + \frac{x}{2v}, \text{ for some } v \in \mathbb{Q}.$$

By equalising the equations of A:

$$u^2vmx^4 - vnu^2x^3 - vx + v = uv^2mx^4 - uv^2mx^3 - v^2ur - ux$$

Then

$$v = u$$
$$m = n$$
$$r = \frac{-1}{u^2}$$

The matrix M is given as follow:

$$M = \begin{pmatrix} 4 & 1 & -1 \\ -3 & 1 & 3 \\ 1 & 0 & 3 \end{pmatrix}$$

such that $\det(M) = 25$. *Furthermore,*

$$M \cdot \begin{pmatrix} D_0 \\ D_1 \\ D_2 \end{pmatrix} = \begin{pmatrix} (\phi_1) \\ (\phi_2) \\ (\phi_3) \end{pmatrix}$$

for $\phi_1 = y - A(x)$, $\phi_2 = \frac{y-B(x)}{x^3}$ *and* $\phi_3 = y - C(x)$. *Then the order of* D_0, D_1 *and* D_∞ *divide* 25. *By using magma we obtain that the order of* D_1 *is exactly* 25 *for any* $n, u \in \mathbb{Q}$, *for the given* $A = \dfrac{u\left(nx^3(x-1)+\dfrac{1}{u^2}\right)}{2} - \dfrac{x}{2u}$ *and* $y^2 = A^2(x) + x^4(x-1)$.

In the article of Leprévost, we see several examples of hyperelliptic curves with different torsion orders, by using the 3×3 matrices. We showed a different one in the previous example. However, generalizing cubic torsion in terms of genus is a hard question, and it is conjectured by the writers in [Patterson, Williams & van der Poorten (2008)] that there do not exist hyperelliptic Jacobians that contain a rational torsion divisor of order g^3.

5. Torsion Points of Elliptic Curves Over Cubic and Quartic Number Fields

Assume that $y^2 = f(x)$ defines an elliptic curve where $\deg(f(x)) = 4$. In [Adams & Razar (1980)], it was proved that the continued fraction expansion of $\sqrt{f(x)}$ is periodic if and only if $D_\infty = \infty_1 - \infty_2$ is a torsion point. Moreover it was proved that if the order of D_∞ is N then the period of the continued fraction of $\sqrt{f(x)}$ is $N-1$ if N is odd, $N-1$ or $2(N-1)$ if N is even.

Mazur, [Mazur & Goldfeld (1978)] gave the complete classification of the torsion subgroup of the points of the elliptic curves E over $\mathbb{Q}$, denoted by $E_{\text{tor}}(\mathbb{Q})$ which is isomorphic to one of the following 15 groups:

$$E_{\text{tor}}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & 1 \le n \le 12, n \ne 11 \quad \text{or} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & 1 \le n \le 4 \end{cases}$$

5.1 Cubic Number Fields

Kenku, Momose, Kamienny [Kamienny (1992); Kenku & Momose (1988)], gave the classification of $E_{\text{tor}}(K)$ where E is an elliptic curve defined over K for K is a quadratic extension of $\mathbb{Q}$ as follows:

$$E_{\text{tor}}\,(K) \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 18, n \neq 17 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 6. \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, \quad n \leq n \leq 2, \text{ only if } K = \mathbb{Q}(\sqrt{-3}) \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \text{ , only if } K = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

By looking at the theorem of Adams and Razar and Mazur's classification of $E_{\text{tor}}\,(\mathbb{Q})$, the possible periods of $\sqrt{f(x)}$ are given as follows:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 18, 22\}$$

Van der Poorten (2004) [van der Poorten (2004)] wrote all square free quartic polynomials $f(x)$ over $\mathbb{Q}$ with a square leading coefficients such that the continued fraction expansion of $\sqrt{f(x)}$ is periodic. Moreover it was shown that there is no polynomial over $\mathbb{Q}$ such that the continued fraction expansion of $\sqrt{f(x)}$ is of period 9 or 11. Then all of these periods exist over $\mathbb{Q}$ except 9 and 11 .

Mohammad Sadek(2016) in [Sadek (2016)] wrote all square free quartic polynomials $f(x)$ with a square leading coefficient over some quadratic field K such that the continued fraction expansion of $\sqrt{f(x)}$ is periodic. Moreover he is giving the quadratic number field for which the absolute value of the discriminant is smallest. By considering the classification of $E_{\text{tor}}(K)$ and Adams and Razar, all possible periods are as follows:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 22, 26, 30, 34\}$$

It was shown that all of these periods occur over some quadratic fields.

The classification of $E_{\text{tor}}(K)$ where K is a cubic number field and E is an elliptic curve over K is given by following theorem:

Theorem 5.1 (Derickx, Etropolski, van Hoeij, Morrow & Zureick-Brown (2021)) *Let E be an elliptic curve defined over a cubic number field K, then*

$$E_{tor}\,(K) \cong \begin{cases} \mathbb{Z}/m\mathbb{Z}, \quad 1 \leq m \leq 16 \ \textit{or}\ m = 18, 20, 21 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \quad 1 \leq m \leq 7 \end{cases}$$

The set of all possible periods of the continued fraction expansion of $\sqrt{f(x)}$ are as follows:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 22, 26, 30, 34, 38\}$$

We need to show that all of these periods, except the periods occuring over $\mathbb{Q}$, are realized over a cubic number field, i.e., we will focus on the following set of periods:

$$\{9, 11, 12, 13, 15, 17, 19, 20, 26, 30, 34, 38\}$$

5.1.1 Periods 9 and 11

Theorem 5.2 *The cubic field K given by the polynomial $x^3 - x^2 + 1$ has the smallest $|\Delta|$ over which there are infinitely many quartic polynomials $f(x)$ for which the continued fraction of $\sqrt{f(x)}$ has period 9, and there are infinitely many quartic polynomials $f(x)$ for which the continued fraction of $\sqrt{f(x)}$ has period 11.*

Proof. By Theorem 2.14 if a curve $y^2 = f(x)$ has the point D_∞ which is order 10 then the period of the continued fraction of $\sqrt{f(x)}$ is either 9 or 18. The parametrization of the elliptic curve with a torsion point of order 10 is given in [Kubert (1976)] as follows:

$$E_{b,c} : y^2 + (1-c)xy - by = x^3 - bx^2$$

where

$$(b, c) = \left(\frac{t^3(t-1)(2t-1)}{(t^2-3t+1)^2}, \frac{-t(t-1)(2t-1)}{t^2-3t+1} \right)$$

According to ([Sadek (2016)], Proposition 4.1) the elliptic curve $E_{b,c}$ can be described

by a quartic model given by $y^2=(X^2+u_{10})^2-4v_{10}(X+w_{10})$ where

$$u_{10}(t)=\frac{-4t^6-16t^5+8t^4+8t^3-4t+1}{4(t^2-3t+1)^2},$$
$$v_{10}(t)=-\frac{t^3(t-1)(2t-1)}{(t^2-3t+1)^2},\ w_{10}(t)=\frac{2t^3-2t^2-2t+1}{2(t^2-3t+1)}$$

with $t(t-1)(2t-1)(t^2-3t+1)\neq 0$ and $k_{10}(t)=-4t(t-1)(t^2-3t+1)$, given in ([Sadek (2016)], Theorem 5.1). According to Lemma 2.1 the continued fraction of μy is periodic of period 9 if and only if $k_{10}=1/\mu^2$, see Remark 2.2. This leads to the equation for the Jacobian of an elliptic curve, given by $J_{10}:=-4t(t-1)(t^2-3t+1)$. Then the period of continued fraction expansion of y is 9 if and only if $E_{10}:=y^2=x^3-x^2-x$ has a solution in a cubic field which is not a cusp. We have $E_{10}(K)=\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}^2$, for K is the cubic number field generated by the polynomial x^3-x^2+1. Moreover, $|\Delta(K)|=23$ is the smallest discriminant, over which we have this period of continued fraction expansion of $\sqrt{f(x)}$.
Similarly, by theorem 2.14 if a curve $y^2=f(x)$ has the point D_∞ which is order 12 then the period of the continued fraction of $y^2=f(x)$ is either 11 or 22. The parametrization of the elliptic curve can be found in [Kubert (1976)] as follows: $E_{b,c}: y^2+(1-c)xy-by=x^3-bx^2$ where

$$(b,c)=\left(\frac{t(2t-1)(2t^2-2t+1)(3t^2-3t+1)}{(t-1)^4},-\frac{t(2t-1)(3t^2-3t+1)}{(t-1)^3}\right),$$

where $t(t-1)(2t-1)(2t^2-2t+1)(3t^2-3t+1)\neq 0$. A quartic model for the elliptic curve $E_{b,c}$ on which $\infty^+-\infty^-$ is a point of order 12 is given by $y^2=(X^2+u_{12})^2-4v_{12}(X+w_{12})$ where

$$u_{12}(t)=\frac{12t^8-120t^7+336t^6-468t^5+372t^4-168t^3+36t^2-1}{4(t-1)^6},$$
$$v_{12}(t)=-\frac{t(2t-1)(2t^2-2t+1)(3t^2-3t+1)}{(t-1)^4},\ w_{12}=\frac{6t^4-8t^3+2t^2+2t-1}{2(t-1)^3},$$

with $k_{12}(t)=\dfrac{4t(2t-1)^2(3t^2-3t+1)^3}{(t-1)^{11}}$.

Similarly the period of y is 11 if and only if the elliptic curve E_{12} which obtained from the square-free part of $k_{12}(t)$; $E_{12}: y^2=x^3+x^2+x$ has a point over K which is not a cusp. We have $E_{12}(K)=\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}$, for K is a number field generated by the polynomial x^3-x^2+1 again.

□

F. Najman found the cubic field with the smallest discriminant having it as a torsion of an elliptic curve for every torsion subgroup over the cubic number field, except $\mathbb{Z}/20\mathbb{Z}$, see [Najman (2012)].When examining the set of possible periods in the case of cubic fields, the only periods that do not appear in the quadratic case are 19 and 38. This refers to a torsion point of order 20. However in this case determining the cubic field with the smallest absolute value of the discriminant is a challenging task. For other cases, the necessary conditions were compiled by M. Sadek, [Sadek (2016)], and the fields with the smallest discriminants were identified by Najman, [Najman (2012)]. In summary, bringing all this information together, for all possible periods over cubic fields (except for 19 and 38), the corresponding $\sqrt{f(x)}$ polynomials have been determined, the conditions under which these periods occur have been specified, and the cubic fields with the smallest discriminants realizing them have been computed.

We aim to address our problem within the context of quartic fields. In their unpublished preprint, Derickx and Najman present a torsion order classification for elliptic curves defined over quartic number fields. Our goal is to compute the specific quartic field with the smallest absolute value of the discriminant on which each torsion subgroup resides and subsequently discuss periodic functions.

5.2 Quartic Number Fields

Theorem 5.3 (Derickx & Najman (2024)) *If K varies over all quartic number fields and E varies over all elliptic curves over K, the groups that appear as $E(K)_{tors}$ are exactly the following*

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 1, \cdots, 18, 20, 21, 22, 24,\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, && n = 1, \cdots, 9,\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, && n = 1, \cdots, 3,\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}, && n = 1, 2,\\
&\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}
\end{aligned}$$

We are interested in the torsion orders which does not occur over $\mathbb{Q}$. So the set of torsion subgroups over a quartic number field K but not over $\mathbb{Q}$ is as follows :

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z}, && n = 11, 13, 14 \cdots, 18, 20, 21, 22, 24,\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, && n = 5, \cdots, 9,\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, && n = 1, \cdots, 3,\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}, && n = 1, 2,\\
&\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}
\end{aligned}$$

In the website [LMFDB Collaboration (2025)] we can find the list of the quartic number fields ordered by the absolute value of the discriminant and labeled in order K_i.

K	Polynomial	Disc.	G.	K	Polynomial	Disc.	G.
K_1	$x^4-x^3-x^2+x+1$	$3^2\cdot 13$	D_4	K_{11}	x^4-x-1	-283	S_4
K_2	$x^4-x^3+x^2-x+1$	5^3	C_4	K_{12}	x^4-2x^3+2	$2^6\cdot 5$	D_4
K_3	x^4-x^2+1	$2^4\cdot 3^2$	C_2^2	K_{13}	$x^4-x^3+x^2+x-1$	-331	S_4
K_4	x^4-x^3+2x+1	$3^3\cdot 7$	D_4	K_{14}	$x^4-x^3-2x^2+3$	$3^2\cdot 37$	D_4
K_5	$x^4-x^3+2x^2+x+1$	$3^2\cdot 5^2$	C_2^2	K_{15}	x^4-x^3+x+1	$2^3\cdot 7^2$	D_4
K_6	x^4-x+1	229	S_4	K_{16}	x^4-x^2-1	$-2^4\cdot 5^2$	D_4
K_7	x^4+1	2^8	C_2^2	K_{17}	x^4+3x^2+1	$2^4\cdot 5^2$	C_2^2
K_8	x^4+x^2-x+1	257	S_4	K_{18}	x^4-3x^2+3	$2^4\cdot 3^3$	D_4
K_9	x^4+x^2-2x+1	$2^4\cdot 17$	D_4	K_{19}	$x^4-x^3-x^2-2x+4$	$3^2\cdot 7^2$	C_2^2
K_{10}	x^4-x^3+2x-1	$-5^2\cdot 11$	D_4	K_{20}	$x^4-2x^3+x^2-2x+1$	$-2^6\cdot 7$	D_4

In this section, we aim to identify, for a given group G in the list of torsion groups given in Theorem 5.3, the quartic field K with the smallest absolute discriminant such that G appears as a torsion group of some elliptic curve $E(K)$. Our work involves examining fields in increasing order of $|\Delta(K)|$. For each field, we either find an elliptic curve with the specified torsion group or prove that no such curve exists. We refer to the field associated with a group G in the list as $K(G)$.

Our strategy centers around examining the arithmetic properties of modular curves $X1(m,mn)$ where $m,n\geq 1$. We are looking for the points of each modular curve over the quartic number fields in the given order of the table. If the modular curve is an elliptic curve finding the points on a number field is straightforward thanks to Magma. If the modular curve is a hyperelliptic curve again, we can use Magma to compute the points; however, in this case, determining the number field is not as straightforward. If the modular curve is neither an elliptic curve nor a hyperelliptic curve we have some tools for deciding which number fields these torsion orders do not occur. But we can not decide the existence of these torsion subgroups by using the strategies we know. We further investigate the newly discovered points to determine whether they generate elliptic curves with the desired torsion structures. This involves analyzing whether the new points correspond to an elliptic curve whose torsion subgroup matches the required order.
In the website [Sutherland (2025b)], respectively [Sutherland (2025a)], we can find that the table provides links to the optimized equations $f(x,y)=0$ for $X_1(N)$,

respectively $X_1(m,mn)$, together with parameterizations.

Let

$$E = [a_1(u,v), a_2(u,v), a_3(u,v), a_4(u,v), a_6(u,v)]$$

$P = [P_x(u,v), P_y(u,v)]$, and $Q = [Q_x(u,v), Q_y(u,v)]$ define an elliptic curve in Weierstrass form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where P is a point of order N, respectively P is a point of order m and Q is a point of order mn on the curve.

5.2.1 Genus 0 Curves

The curve $X_1(m,mn)$ is defined over the cyclotomic field $\mathbb{Q}(\zeta_m)$. Then first, we look at the existence of ζ_m in the number field K. If it exists, we search the non-cusp points over the modular curve $X_1(m,mn)$ on K. Then we evaluate all the points on the corresponding elliptic curve, if one point gives us the wanted torsion order, we are done.

Theorem 5.4 *The genus* 0 *modular curves and their corresponding number field with the smallest absolute value of the discriminant are as follows:*

- $K(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = K_1$
- $K(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}) = K_1$
- $K(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) = K_3$
- $K(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) = K_2$

Proof. Magma was utilized for these calculations. If you would like more details about the curve equations, you can find some of them in the thesis [Kazancıoğlu (2023)] and [Kazancıoğlu & Sadek (2025)]

Since K_1 contains ζ_3, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ can occur over K_1. The corresponding elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is given as $y^2 + y = x^3$ where the point is $(0, \zeta_3)$. Corresponding elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is given as $y^2 + (2\zeta_3 + 1)xy + (6\zeta_3 + 4)y = x^3 + (6\zeta_3 + 4)x^2$ where the point is $(0, \zeta_3)$. Since K_1 does not contain ζ_4 and ζ_5, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ do not occur as a torsion subgroup of an elliptic curve over K_1.

Since K_2 does not contain ζ_4, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ cannot occur as a torsion subgroup of an elliptic curve over K_2. Notice that K_2 contains ζ_5, so it is enough to find one elliptic curve with torsion $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ over K_2.

The corresponding elliptic curve with torsion $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ is given by $y^2+\frac{1}{22}\left(-8\zeta_5^3+5\zeta_5^2-8\zeta_5+24\right)xy+\frac{1}{22}\left(-8\zeta_5^3+5\zeta_5^2-8\zeta_5+2\right)y=x^3+\frac{1}{22}\left(-8\zeta_5^3+5\zeta_5^2--8\zeta_5+2\right)x^2$ where the point is $(0,\zeta_5)$.

K_3 contains ζ_4 and the corresponding elliptic curve over K_3 is given by $y^2+xy+\frac{1}{2}\left(3\zeta_4+1\right)y=x^3+\frac{1}{2}\left(3\zeta_4+1\right)x^2$ where the point is $(0,\zeta_4)$. □

5.2.2 Genus 1 Curves

Genus 1 curves are elliptic curves and Magma can compute their Mordell-Weil group over any number field. Here, if the Mordell-Weil Group is different from the Mordell-Weil Group over $\mathbb{Q}$ then there may be a non-cusp point over K. We evaluate the points on the related elliptic curve; if it gives us the wanted torsion group, we are done.

Theorem 5.5 *The genus* 1 *modular curves and their corresponding number field with the smallest absolute value of the discriminant are as follows:*

- $K(\mathbb{Z}/11\mathbb{Z})=K_1$
- $K(\mathbb{Z}/14\mathbb{Z})=K_3$
- $K(\mathbb{Z}/15\mathbb{Z})=K_2$
- $K(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z})=K_1$
- $K(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z})=K_4$
- $K(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z})=K_5$
- $K(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z})=K_{17}$
- $K(\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z})=K_{19}$

Proof. The modular curve $X_1(11)$ is given in the table or can be given by the equation $y^2-y=x^3-x^2$. The Mordell Weil Group of this curve over K_1 is isomorphic to $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}$. The point $(-a^2+1,a+1)$ is one of the infinite order points which gives us the elliptic curve $y^2+(-a^3-3a^2-a+1)xy+(-4a^3-4a^2+1)y=$

$x^3+(-4a^3+a^2+7a+4)x^2$ over K_1 which has a torsion subgroup $\mathbb{Z}/11\mathbb{Z}$.

$X_1(14)(K_1) \cong X_1(14)(K_2) \cong X_1(14)(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$, so all points are cusps over K_1 and K_2 also. $X_1(14)(K_3) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$. The point $(-a^2+a, -a^3+a^2+a-2)$ has an infinite order which gives us an elliptic curve over K_3 as follows:

$y^2 + 1/13(9a^3 - 11a^2 + 3a + 18)xy + 1/169(60a^3 - 43a^2 - 32a + 68)y = x^3 + 1/169(60a^3-43a^2-32a+68)x^2$

$X_1(15)(K_1) \cong X_1(15)(\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}$, so all the points over K_1 are cusps. However, $X_1(15)(K_2) \cong \mathbb{Z}/16\mathbb{Z}$, and the point $(a-1, -a^3+a^2-a)$ gives us an elliptic curves $y^2+(-2a^3+5a^2-5a+3)xy+(3a^3+5a^2-13a+10)y = x^3+(3a^3+5a^2-13a+10)x^2$ over K_2 with torsion order $\mathbb{Z}/15\mathbb{Z}$.

$X_1(2,10)(K_1) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$. The point $(2a^3-3a^2+2, -3a^3+5a^2-a-2)$ has an infinite order which gives us an elliptic curve over K_1 with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ as follows:

$y^2 = x^3 + 1/14523721(-1744472a^3 - 6669240a^2 + 13343304a - 2211914)x^2 + 1/210938471685841(-18346356787928a^3 + 33511461110808a^2 - 33122427523848a + 18185366189609)x$

$X_1(2,12)(K_1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, but all the points are either cusps or make the curve singular, so there is no torsion subgroup of the wanted order. $X_1(2,12)(K_2) \cong X_1(2,12)(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$, then all points are cusps. $X_1(2,12)(K_3) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, but all the points make the curve singular. $X_1(2,12)(K_4) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$, and one of the infinite order point $(4a^3-6a^2+3a+7, 8a^3-13a^2+8a+12)$ gives us an elliptic curve which has a torsion subgroup of order $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ as follows:

$$\begin{aligned} y^2 &= x^3 + 1/8296707(25496368a^3 - 43679680a^2 + 33284048a + 28964434)x^2 \\ &+ 1/22945115681283(-57628102792176a^3 + 89094520329664a^2 \\ &- 45974145521936a - 96546884975333)x \end{aligned}$$

$X_1(3,9)(K_1) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ but the points are either cusps or give us singular curves. K_2 does not contain ζ_3. $X_1(3,9)(K_3) \cong X_1(3,9)(K_4) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ but the points are either cusps or give us singular curves or give us the curves with the torsion group isomorphic to $\mathbb{Z}/9\mathbb{Z}$. On the other hand, $X_1(3,9)(K_5) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ and one of the infinite order point $(1/4(a^3-a^2+3a+5), 1/8(3a^3-3a^2+9a+7))$ gives

us an elliptic curve which has a torsion subgroup of order $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ defined by

$$\begin{aligned} & y^2+1/61731(-394a^3+394a^2-1182a+69205)xy \\ + \;& 1/66854673(-270034a^3+270034a^2-810102a+6932362)y \\ = \;& x^3+1/66854673(-270034a^3+270034a^2-810102a+6932362)x^2 \end{aligned}$$

$K_1, K_2, K_4, K_5, K_6, K_8, K_{10}, K_{11}, K_{13}, K_{14}, K_{15}, K_{16}$ do not contain ζ_4. $X_1(4,8)(K_3) \cong X_1(4,8)(K_9) \cong X_1(4,8)(K_{12}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and $X_1(4,8)(K_7) \cong \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ but the points are either cusps or give us singular curves. $X_1(4,8)(K_{17}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ and one of the infinite order points $(5a^3+2a, -15a^3-24a^2-6a-9)$ gives an elliptic curve with a torsion subgroup $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ over K_{17} as follows:

$$y^2+xy-410y = x^3-410x^2$$

$K_2, K_6, \cdots, K_{13}, K_{15}, K_{16}, K_{17}$ do not contain ζ_6. $X_1(6,6)(K_1) \cong X_1(6,6)(K_3) \cong X_1(6,6)(K_4) \cong X_1(6,6)(K_5) \cong X_1(6,6)(K_{14}) \cong X_1(6,6)(K_{18}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ but the points are either cusps or give us singular curves.

$X_1(6,6)(K_{19}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ and one of the infinite order points (a^3-2, a^3-3) gives an elliptic curve with a torsion subgroup $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ over K_{19} as follows:

$$y^2+(9a^3+90)xy+(13122a^3+104976)y = x^3+(162a^3+1296)x^2$$

□

5.2.3 Genus 2 Curves

Genus 2 curves can be hyperelliptic or non-hyperelliptic, and Magma can compute the points of the curve over any number field. The points may be non-cusp points over K. We evaluate the points on the related elliptic curve; if it gives us the wanted torsion group, we are done. From the data's of Andrew V. Sutherland, we obtain the unsimplifed version of the curves and by using Magma we transfer them in a simplified version if it is an hyperelliptic curve, i.e. the form of $y^2 = f(x)$ where $f(x)$ is a polynomial of the degree $2g+1$ or $2g+2$.

Theorem 5.6 *The genus* 2 *modular curves and their corresponding number field with the smallest absolute value of the discriminant are as follows:*

- $K(\mathbb{Z}/13\mathbb{Z}) = K_1$
- $K(\mathbb{Z}/16\mathbb{Z}) = K_2$
- $K(\mathbb{Z}/18\mathbb{Z}) = K_8$

Proof. $X_1(13) := y^2 + (x^3 + x^2 + 1)y - x^2 - x$, and the simplified form can be given as $y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$. We find the points of simplified form over K_1 via Magma and pull back on the unsimplified form. Then one of the points $(-a^3 + a^2 - 1, -a^2)$ gives us an elliptic curve over K_1 with the desired torsion subgroup $\mathbb{Z}/13\mathbb{Z}$ as follows:

$y^2 + (2a^3 - 2a)xy + (3a^3 + 2a^2 - a - 1)y = x^3 + (3a^3 + 2a^2 - a - 1)x^2$.

$X_1(16) := y^2 + (x^3 + x^2 - x + 1)y + x^2$, and the simplified form can be given as $y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$. In Magma, to identify the points of a hyperelliptic curve, we must set a bound. However, we believe that the points found within this bound are sufficient to determine the number fields. The points we have found on the curve, within the specified bound, are all cusps over K_1. However, over K_2 the point $(1/11(10a^3 - 10a^2 - 7), 1/1331(812a^3 - 344a^2 + 876a - 1625))$ gives us an elliptic curve as follows:

$y^2 + 1/483153(1488897a^3 + 435511a^2 + 1235306a + 116480)xy + 1/1929229929(-3387895251a^3 + 296044677a^2 - 1836840618a + 2768924824)y = x^3 + 1/1929229929(-3387895251a^3 + 296044677a^2 - 1836840618a + 2768924824)x^2$

where it has the desired torsion subgroup $\mathbb{Z}/16\mathbb{Z}$.

$X_1(18) := y^2 + (x^3 - 2x^2 + 3x + 1)y + 2x$ and the simplified form can be given as $y^2 = x^6 - 4x^5 + 10x^4 - 10x^3 + 5x^2 - 2x + 1$. We have the same situation with the previous case here. Over K_2, K_6, K_7 all points we have found on the curve, within the specified bound, are all cusps. Over K_1, K_3, K_4, K_5 we have non-cusp points, yet they give only singular curve. But over K_8 the point $(1/2(-a^3 - a^2 + 1), 1/8(3a^3 + a^2 - 2a - 9))$ gives us an elliptic curve as follows:

$y^2 + 1/19(-61a^3 - 58a^2 - 85a + 35)xy + 1/361(499a^3 + 595a^2 + 833a + 113)y = x^3 + 1/361(499a^3 + 595a^2 + 833a + 113)x^2$

with the desired torsion subgroup $\mathbb{Z}/18\mathbb{Z}$.

□

5.2.4 Higher Genus Curves

The rest of the curves are given as follows:

- Genus 3: $X_1(20)$
- Genus 4: $X_1(2,14)$
- Genus 5: $X_1(17), X_1(21), X_1(24), X_1(2,16)$
- Genus 6: $X_1(22)$
- Genus 7: $X_1(2,18)$

All of these algebraic curves are non-hyperelliptic curves. By using Magma we can not compute the points of an algebraic curve if it is not an elliptic or hyperelliptic curve. We can use some tools to obtain an idea about the existence of this torsion subgroup over a quartic number field.

First, instead of looking the points of $X_1(20)$ over a number field K, we can search the points of $X_0(20)$. Some of the Modular curves $X_0(N)$ can be found in the web site [The LMFDB Collaboration (2024)]. Since $X_0(20)$ is an elliptic curve, it is easy to compute its Mordell-Weil group via Magma. If all the points of $X_0(20)$ is cusp, there is no 20 cycle over K. By this idea we can eliminate the quartic number fields as follows: $K_2, K_4, K_6, K_{10}, K_{11}, K_{15}, K_{19}, K_{20}$, since their Mordell Weil groups is somorphic to the $\mathbb{Z}/6\mathbb{Z}$, which is the same over $\mathbb{Q}$. We know that $X_0(4n)$ has 6 rational cusps for n is a prime number, see [Ogg (1972)]. Then all of the points are cusps over these number fields. For the rest of the number fields, 20-cycle may exist.

Moreover, we know that $X_1(4n)$ covers $X_1(2,2n)$, then we can check the existence of non-cusp points of $X_1(2,2n)$, which is an elliptic curve in the case $n=5$. Then we check the Mordell-Weil group of $X_1(2,10)$ over the given 20 number fields and, we could eliminate the number fields $K_3, K_4, K_6, K_{11}, K_{15}, K_{19}, K_{20}$, since the Mordell-Weil group over these number fields is isomorphic to $\mathbb{Z}/6\mathbb{Z}$, which is the same over $\mathbb{Q}$. So in general there is no 20-cycle over the number fields as follows:

$$K_2, K_3, K_4, K_6, K_{10}, K_{11}, K_{15}, K_{19}, K_{20}$$

BIBLIOGRAPHY

Adams, W. W. & Razar, M. J. (1980). Multiples of points on elliptic curves and continued fractions. *Proceedings of the London Mathematical Society*, *3*(3), 481–498.

Bernard, N., Leprévost, F., & Pohst, M. (2009). Jacobians of genus-2 curves with a rational point of order 11. *Experimental Mathematics*, *18*(1), 65–70.

Berry, T. G. (1990). On periodicity of continued fractions in hyperelliptic function fields. *Archiv der Mathematik*, *55*, 259–266.

Bosma, W., Cannon, J., & Playoust, C. (1997). The magma algebra system i: The user language. *Journal of Symbolic Computation*, *24*(3-4), 235–265.

Derickx, M., Etropolski, A., van Hoeij, M., Morrow, J. S., & Zureick-Brown, D. (2021). Sporadic cubic torsion. *Algebra & Number Theory*, *15*(7), 1837–1864.

Derickx, M. & Najman, F. (2024). Classification of torsion of elliptic curves over quartic fields. *arXiv preprint arXiv:2412.16016*.

Faltings, G. (1986). Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry* (pp. 9–26). Springer.

Flynn, E. V. (1990). Large rational torsion on abelian varieties. *Journal of Number Theory*, *36*(3), 257–265.

Flynn, E. V. (1991). Sequences of rational torsions on abelian varieties. *Inventiones mathematicae*, *106*, 433–442.

Hardy, G. H. & Wright, E. M. (1979). *An introduction to the theory of numbers*. Oxford university press.

Jeon, D., Kim, C. H., & Schweizer, A. (2004). On the torsion of elliptic curves over cubic number fields. *Acta Arithmetica*, *113*, 291–301.

Kamienny, S. (1992). Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. math*, *109*(2), 221–229.

Kazancıoğlu, M. U. & Sadek, M. (2025). On torsion subgroups of elliptic curves over quartic, quintic and sextic number fields. *Journal of Number Theory*, *274*, 37–55.

Kazancıoğlu, M. U. (2023). Torsion structure of elliptic curves over small number fields. Master's thesis, Sabancı University.

Kenku, M. A. & Momose, F. (1988). Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, *109*, 125–149.

Kubert, D. S. (1976). Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society*, *3*(2), 193–237.

Leprévost, F. (1991). Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, *313*(11), 771–774.

Leprévost, F. (1992). Torsion sur des familles de courbes de genre g. *Manuscripta mathematica*, *75*, 303–326.

Leprévost, F. (1995). Jacobiennes de certaines courbes de genre 2: torsion et simplicité. *Journal de théorie des nombres de Bordeaux*, *7*(1), 283–306.

Leprévost, F. (1996). Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, *1996*(473), 59–68.

Leprévost, F. (1997). Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre g 1. *manuscripta mathematica*, *92*, 47–63.

Liu, Q. (1996). Modeles entiers des courbes hyperelliptiques sur un corps de valuation discrete. *Transactions of the American Mathematical Society*, *348*(11), 4577–4610.

LMFDB Collaboration, T. (2025). The L-functions and modular forms database. `https://www.lmfdb.org`. [Online; accessed 7 May 2025].

Lockhart, P. (1994). On the discriminant of a hyperelliptic curve. *Transactions of the American Mathematical Society*, *342*(2), 729–752.

Mazur, B. & Goldfeld, D. (1978). Rational isogenies of prime degree. *Inventiones mathematicae*, *44*, 129–162.

Merel, L. (1996). Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, *124*(1), 437–450.

Najman, F. (2012). Torsion of elliptic curves over cubic fields. *Journal of number theory*, *132*(1), 26–36.

Nicholls, C. (2018). *Descent methods and torsion on Jacobians of higher genus curves*. PhD thesis, University of Oxford.

Nicol, M. & Petersen, K. (2023). Ergodic theory: basic examples and constructions. In *Ergodic theory* (pp. 3–34). Springer.

Ogg, A. (1972). Rational points on certain elliptic modular curves. In *AMS Conference, St. Louis, 1972*, (pp. 211–231).

Patterson, R. D., Williams, H. C., & van der Poorten, A. J. (2008). Sequences of jacobian varieties with torsion divisors of quadratic order. *Functiones et Approximatio Commentarii Mathematici*, *39*(2), 345–360.

Sadek, M. (2016). Periodic continued fractions and elliptic curves over quadratic fields. *Journal of Symbolic Computation*, *76*, 200–218.

Silverman, J. H. (2009). *The arithmetic of elliptic curves*, volume 106. Springer.

Stichtenoth, H. (2009). *Algebraic Function Fields and Codes*. Graduate Texts in Mathematics. Springer Berlin Heidelberg.

Stoll, M. (2014). Arithmetic of hyperelliptic curves. Summer Semester Lecture Notes, University of Bayreuth.

Sutherland, A. V. (2025a). Models for the modular curves $x_1(m,n)$. `https://math.mit.edu/~drew/X1mn.html`. Accessed: 2025-05-07.

Sutherland, A. V. (2025b). Tables of optimal elliptic curves over $\mathbb{Q}$. `https://math.mit.edu/~drew/X1_optcurves.html`. Accessed: 2025-05-07.

The LMFDB Collaboration (2024). Knowledge: Modular curve $x_0(n)$ — lmfdb. `https://www.lmfdb.org/knowledge/show/ag.modcurve.x0`. Online; accessed 12 May 2025.

van der Poorten, A. J. (2004). Periodic continued fractions and elliptic curves. In *International Conference in Number Theory in Honour of Hugh Williams on his 60th Birthday*, (pp. 353–365). American Mathematical Society.

Van der Poorten, A. J. & Tran, X. C. (2000). Quasi-elliptic integrals and periodic continued fractions. *Monatshefte für Mathematik*, *131*(2), 155–169.

Zarhin, Y. G. (1999). Hyperelliptic jacobians without complex multiplication. *arXiv preprint math/9909052*.